PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-085048
(43)Date of publication of application : 20.03.2003

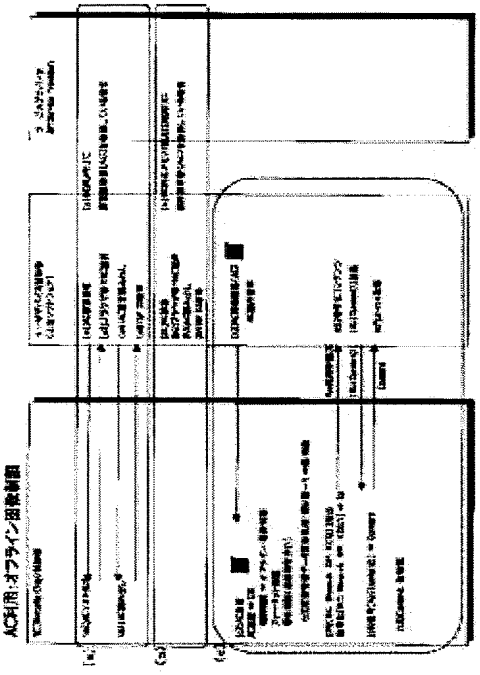
(51)Int.Cl. G06F 12/14
G06F 12/00
G06F 12/16
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 2001-274746
(22)Date of filing : 11.09.2001

(71)Applicant : SONY CORP
(72)Inventor : SHIMADA NOBORU
ISHIBASHI YOSHITO
ABE HIROSHI
OKA MAKOTO

(54) BACKUP DATA MANAGEMENT SYSTEM, BACKUP DATA MANAGEMENT METHOD, AND INFORMATION PROCESSING DEVICE, AND COMPUTER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system capable of executing backup data management in an information processing device securely and efficiently.
SOLUTION: Backup object data are enciphered by a backup key, and enciphered key data acquired by enciphering the backup key by using a public key of a support center which is an external entity are generated, and the generated data are stored in media or transmitted to the support center. In restore processing of the backup data, a partitioned region is set in a memory in the information processing device following an attribute certificate for memory region security, and the data are stored. Hereby, there is no possibility of being decoded even if a backup data storage medium is transferred to a third party, to thereby reduce the load of the backup data management in a user device, and to facilitate management under high grade security of the data.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－85048
（P2003－85048A）
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.[7]		識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
	12/00	５３１	12/00	５３１Ｍ	５Ｂ０１８
	12/16	３１０	12/16	３１０Ｍ	５Ｂ０８２
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｊ１０４
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	

審査請求　未請求　請求項の数15　ＯＬ　（全 82 頁）　最終頁に続く

(21)出願番号　特願2001－274746(P2001－274746)

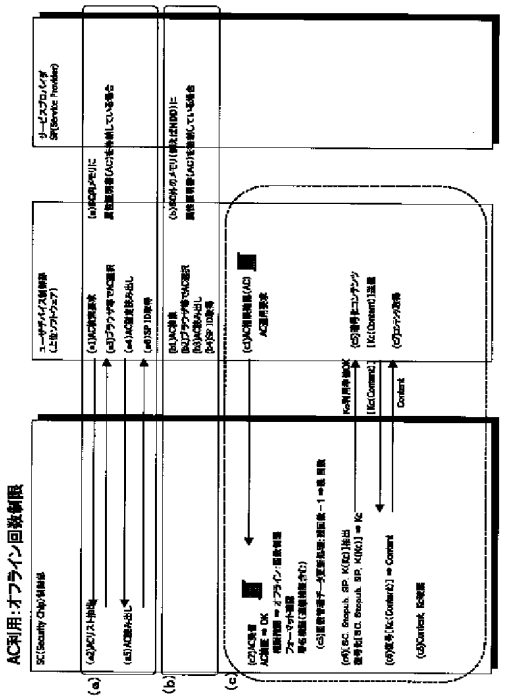
(22)出願日　平成13年９月11日(2001.9.11)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　島田　昇
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　バックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラム

(57)【要約】
【課題】　情報処理装置におけるバックアップデータ管理をセキュアにかつ効率的に実行可能としたシステムを実現する。
【解決手段】　バックアップ対象データをバックアップ鍵で暗号化するとともに、バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成し、生成データをメディアに格納、またはサポートセンタに送信する。バックアップデータのリストア処理は、メモリ領域確保用属性証明書に従って情報処理装置のメモリに区分領域を設定し、格納する。第三者にバックアップデータ格納メディアが渡ったとしても復号される恐れがなく、ユーザデバイスにおけるバックアップデータ管理の負担が軽減され、データの高度なセキュリティの下での管理が容易となる。



1

【特許請求の範囲】
【請求項１】情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理システムであり、
前記情報処理装置は、
バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティテイであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有し、
前記サポートセンタは、該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行する構成を有することを特徴とするバックアップデータ管理システム。
【請求項２】前記情報処理装置は、
前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする請求項１に記載のバックアップデータ管理システム。
【請求項３】前記サポートセンタは、
バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行する構成であることを特徴とする請求項１に記載のバックアップデータ管理システム。
【請求項４】前記バックアップ対象データは、
前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、
前記情報処理装置は、メモリ領域確保用属性証明書に記録された領域確保条件に従って、前記メモリ内に区分領域を設定する処理を実行する構成を有し、
前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、
前記情報処理装置は、
前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする請求項１に記載のバックアップデータ管理システム。
【請求項５】前記情報処理装置は、
メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に

2

前記バックアップデータを格納する処理を実行する構成を有し、
前記情報処理装置は、
前記メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行する構成であることを特徴とする請求項１に記載のバックアップデータ管理システム。
【請求項６】情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理方法であり、
前記情報処理装置において、
バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティテイであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信し、
前記サポートセンタにおいて、
該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行することを特徴とするバックアップデータ管理方法。
【請求項７】前記情報処理装置は、
前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行することを特徴とする請求項６に記載のバックアップデータ管理方法。
【請求項８】前記サポートセンタは、
バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行することを特徴とする請求項６に記載のバックアップデータ管理方法。
【請求項９】前記バックアップ対象データは、
前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、
前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、
前記情報処理装置は、
前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行することを特徴とする請求項６に記載のバックアップデータ

管理方法。
【請求項１０】前記情報処理装置は、
メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行することを特徴とする請求項６に記載のバックアップデータ管理方法。
【請求項１１】データ処理を実行する情報処理装置であり、
バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有することを特徴とする情報処理装置。
【請求項１２】前記情報処理装置は、
前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする請求項１１に記載の情報処理装置。
【請求項１３】前記バックアップ対象データは、
前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、
前記情報処理装置は、
メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする請求項１１に記載の情報処理装置。
【請求項１４】前記情報処理装置は、
メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行する構成であることを特徴とする請求項１１に記載の情報処理装置。
【請求項１５】情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、
バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータを生成するステップと、
前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成するステップと、
を有することを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、バックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムに関する。特に、情報処理装置におけるデータ処理の開始条件として設定されるパスワードの管理を、セキュアにかつ効率的に実行することを可能としたバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムに関する。
【０００２】
【従来の技術】昨今、音楽データ、画像データ、ゲームプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット、衛星を介した通信他、有線、無線の各種通信網を介して配信するサービスが盛んになってきている。また、ＤＶＤ、ＣＤ、メモリカード等の流通可能な記憶媒体を介したコンテンツ流通も盛んになってきている。これらの流通コンテンツは、ユーザの所有する例えば、ＴＶ、ＰＣ（Personal Computer）、再生専用器、あるいはゲーム機器等において、再生、利用される。
【０００３】通信網を介して配信されるコンテンツは、例えば通信機能を有するセットトップボックスによって受信され、ＴＶ他の再生装置において再生可能なデータに変換されて再生されたり、あるいは通信インタフェースを備えたＴＶ、再生装置、ゲーム機器、ＰＣ等の情報機器によって受信されて再生される。
【０００４】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。
【０００５】ユーザに対する利用制限を実現する１つの手法が、配布コンテンツの暗号化処理である。例えば著作権保護の要請されるコンテンツを衛星通信あるいはインターネット通信等を介した配信、あるいはＤＶＤ等のメディアに格納して配布する場合にコンテンツを暗号化して配信または格納し、正規ユーザに対してのみコンテンツ復号に利用可能な復号鍵を配布する。正規ユーザは配布された復号鍵によって暗号化コンテンツの復号を実行し、コンテンツを再生する構成である。
【０００６】暗号化データは、復号鍵を用いた復号化処理によって復号データ（平文）に戻すことができる。データ暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。
【０００７】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式

5

がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Data encryption standard）がある。

【０００８】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【０００９】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なる鍵で行なう方式がいわゆる公開鍵暗号方式と呼ばれる方式である。公開鍵暗号方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が生成した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号化処理が可能となる。秘密鍵は、公開鍵を生成した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号方式の代表的なものには、楕円曲線暗号、あるいはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【００１０】

【発明が解決しようとする課題】上記のようなコンテンツ利用管理システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはＤＶＤ、ＣＤ等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツ鍵を正当なユーザにのみ提供する構成が多く採用されている。コンテンツ鍵自体の不正な利用等を防ぐためのコンテンツ鍵を暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツ鍵を復号してコンテンツ鍵を使用可能とする構成が提案されている。

【００１１】正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツ鍵の配信前に認証処理を実行することによって行なう。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツ鍵を暗号化して通信を行なう。

6

【００１２】例えば上述の認証処理に必要な鍵データ、ユーザデバイスＩＤなどのデータは第三者に漏洩することのないように管理することが必要となる。従って、このような秘密データは第三者によるアクセスがなされないよう、パスワード等によってアクセス権を確認することが行なわれる。

【００１３】しかし、このような秘密情報は、例えばユーザデバイスの故障等によりアクセスが不能となる場合に備えて何らかのメディアにバックアップデータとして格納しておくことが必要となる場合がある。ただし、バックアップデータに基づくデータ漏洩を考慮した場合、暗号化処理を行なった上でバックアップを行なうことが好ましいが、デバイスから取り出せる鍵を用いた暗号化処理を行なうと、不正な第三者によって鍵が取得され、機密データが復号されて漏洩する可能性がある。

【００１４】本発明は、上述の問題点に鑑みてなされたものであり、バックアップデータの管理におけるユーザの負担を軽減し、バックアップデータの漏洩防止を図り、さらに、バックアップデータに基づくリストア処理も効率的にかつセキュアに実行することを可能としたバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムを提供することを目的とする。

【００１５】

【課題を解決するための手段】本発明の第１の側面は、情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理システムであり、前記情報処理装置は、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有し、前記サポートセンタは、該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行する構成を有することを特徴とするバックアップデータ管理システムにある。

【００１６】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記情報処理装置は、前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする。

【００１７】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記サポートセンタは、バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行する構成であることを特徴とする。

【００１８】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、前記情報処理装置は、メモリ領域確保用属性証明書に記録された領域確保条件に従って、前記メモリ内に区分領域を設定する処理を実行する構成を有し、前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、前記情報処理装置は、前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする。

【００１９】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記情報処理装置は、メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有し、前記情報処理装置は、前記メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行する構成であることを特徴とする。

【００２０】さらに、本発明の第２の側面は、情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理方法であり、前記情報処理装置において、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信し、前記サポートセンタにおいて、該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行することを特徴とするバックアップデータ管理方法にある。

【００２１】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記情報処理装置は、前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行することを特徴とする。

【００２２】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記サポートセンタは、バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行することを特徴とする。

【００２３】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、前記情報処理装置は、前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行することを特徴とする。

【００２４】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記情報処理装置は、メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行することを特徴とする。

【００２５】さらに、本発明の第３の側面は、データ処理を実行する情報処理装置であり、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有することを特徴とする情報処理装置にある。

【００２６】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする。

【００２７】さらに、本発明の情報処理装置の一実施態様において、前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、前記情報処理装置は、メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする。

【００２８】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行する構成であることを特徴とする。

【００２９】さらに、本発明の第４の側面は、情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータを生成するステップと、前記バックアップ鍵を外部エンティテイであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成するステップと、を有することを特徴とするコンピュータ・プログラムにある。

【００３０】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００３１】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００３２】

【発明の実施の形態】［システム概要］図１に本発明のコンテンツ利用管理システムにおける各エンティテイ、および各エンティテイの処理の概要を説明する図を示す。

【００３３】ユーザデバイス１０１は、コンテンツを利用する各ユーザの端末であり、具体的には、ＰＣ、ゲーム端末、ＤＶＤ，ＣＤ等の再生装置、記録再生装置等である。これらの端末には、後段で説明する暗号処理、コンテンツ利用処理を制御する制御手段を備えた耐タンパ構成のセキュリティチップが装着されている。コンテンツ配信エンティテイ（コンテンツディストリビュータ）としてのサービスプロバイダ（ＳＰ－ＣＤ）１０２、その他のエンティテイとユーザデバイス１０１間で実行されるデータ転送等におけるユーザデバイス１０１側のセキュアな処理の多くは、セキュリティチップ内で制御、実行される。

【００３４】サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２は、セキュリティチップを持つユーザデバイス１０１に対してコンテンツを提供するサービスプロバイダである。コンテンツクリエータ１０３は、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２に対してサービスに供するためのコンテンツを提供する。ユーザデバイス製造者（Manufacturer）１０４は、ユーザデバイス１０１を製造するエンティテイである。

【００３５】サポートセンタ１０５は、ユーザデバイス１０１に装着されたユーザデバイスでの様々な処理に対するサポートを実行するセンタであり、例えばユーザが認証情報として利用するパスワードを忘れた場合のパスワードのリカバリ処理、あるいはユーザデバイスが生成したコンテンツのバックアップデータを利用したリストア（復旧）処理など、ユーザデバイスに対する様々なサポート処理を実行する。認証局（ＣＡ：Certification Authority）１０６は各エンティテイに対して公開鍵証明書(ＰＫＣ：Public Key Certificate)を発行する。

【００３６】なお、ユーザデバイス１０１、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２、コンテンツクリエータ１０３、ユーザデバイス製造者（Manufacturer）１０４、サポートセンタ１０５、認証局（ＣＡ：Certification Authority）１０６、各エンティテイの数は任意である。特に、図１において、認証局（ＣＡ：Certification Authority）１０６を１つのみ示してあるが、認証局は、各エンティテイでの処理に応じて必要となる公開鍵証明書を発行する複数の認証局が存在してよい。

【００３７】ユーザデバイス１０１は、衛星通信、インターネット通信、あるいはその他、有線、無線のデータ通信ネットワークを介してサービスプロバイダ（コンテンツディストリビュータ）１０２から暗号化されたコンテンツを受信し、コンテンツを利用する。暗号化コンテンツを復号するための鍵：コンテンツ鍵：Ｋｃは暗号化されてコンテンツ利用権限を示す権限情報証明書としてのコンテンツ利用権限証明書、例えば属性証明書（ＡＣ：Attribute Certificate）１１０に格納されており、ユーザ端末１０１がコンテンツを復号して利用するためには、サービスプロバイダ（コンテンツディストリビュータ）１０２から属性証明書（ＡＣ：Attribute Certificate）１１０を受領し、セキュリティチップを持つユーザデバイスにおいて属性証明書から鍵を取り出して復号することが必要となる。

【００３８】コンテンツ利用権限を示す権限情報証明書としてのコンテンツ利用権限証明書、例えば属性証明書（ＡＣ：Attribute Certificate）１１０には、暗号化されたコンテンツ鍵：Ｋｃの他に、コンテンツの利用制限回数や利用期限など、コンテンツの利用制限情報が記録されており、ユーザデバイス１０１は、コンテンツ利用権限証明書としての属性証明書（ＡＣ）１１０に記録されたコンテンツ利用制限に従ったコンテンツの利用が

可能となる。

【００３９】なお、以下、実施例の説明では、属性証明書（ＡＣ：Attribute Certificate）１１０にコンテンツの利用情報、暗号化コンテンツ鍵を格納した構成として説明するが、コンテンツの利用情報、暗号化コンテンツ鍵を格納した証明書は、いわゆる規定に従った属性証明書（ＡＣ）に限らず、任意のデータフォーマットの証明書として構成可能である。すなわちコンテンツの利用権限を証明するデータを格納し、データ改竄検証のための発行エンティテイの署名データが付加された構成であれば、任意のデータ形式のコンテンツ利用権限証明書が利用可能である。

【００４０】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。

【００４１】図１で示す各エンティテイ中、認証局１０６以外のエンティテイ、すなわちユーザデバイス１０１、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２、コンテンツクリエータ１０３、およびユーザデバイス製造者（Manufacturer）１０４、サポートセンタ１０５のエンティテイは、所定のルールに従ってコンテンツ利用、コンテンツ配信を可能とするため、各エンティテイでの処理を所定のルールに従って実行する。このルールを設定し、管理するエンティテイとして図示しないシステムホルダ（ＳＨ:System Holder）がある。図１の１０１～１０５の各エンティテイは、システムホルダ（ＳＨ）の設定したコンテンツ利用インフラ、ルールの下で各エンティテイでの処理を実行する。

【００４２】例えばユーザデバイス製造者（Manufacturer）１０４は、製造するユーザデバイス内の耐タンパ構成を持つセキュリティチップ内に、コンテンツ配信において適用するデバイス識別子（ＩＤ）、および各種の暗号処理鍵を格納する。ユーザデバイス１０１、サービスプロバイダ（コンテンツディストリビュータ）１０２、コンテンツクリエータ（ＣＣ）１０３、サポートセンタ１０５間でのコンテンツ転送、属性証明書の転送、その他のデータ転送処理においては、システムホルダ（ＳＨ）の設定したルールに基づいて、例えば相互認証処理、データ暗号化処理を実行する。

【００４３】また、ユーザデバイス１０１におけるコンテンツ利用に際しては、属性証明書に記録された利用制限を遵守したコンテンツ利用を実行する。例えば回数制限の設定されたコンテンツの利用に際してデバイス内のセキュリティチップの制御部の制御の下に、コンテンツ利用可能回数を係数するカウンタを更新する処理等を実行する。このような各エンティテイでの処理のルールを規定したプラットホームを構築し、管理するエンティテイがシステムホルダ（ＳＨ）である。

【００４４】［公開鍵証明書，属性証明書］図１の構成において利用される公開鍵証明書、属性証明書について、その概要を説明する。

【００４５】（公開鍵証明書（ＰＫＣ））公開鍵証明書について図２，図３、図４を用いて説明する。公開鍵証明書は、認証局（ＣＡ：Certification Authority）が発行する証明書であり、ユーザ、各エンティテイが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【００４６】公開鍵証明書のフォーマット例を図２～図４に示す。これは、公開鍵証明書フォーマットＩＴＵ－Ｔ　Ｘ．５０９に準拠した例である。

【００４７】バージョン（version）は、証明書フォーマットのバージョンを示す。シリアルナンバ（Serial Number）は、公開鍵証明書発行局（ＣＡ）によって設定される公開鍵証明書のシリアルナンバである。シグネチャ（Signature）は、証明書の署名アルゴリズムである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。発行者（issuer）は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局（ＩＡ）の名称が識別可能な形式（Distinquished Name）で記録されるフィールドである。有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。サブジェクト公開鍵情報(subject Public Key Info)は、証明書所有者の公開鍵情報として鍵のアルゴリズム、鍵が格納される。

【００４８】証明局鍵識別子（authority Key Identifier－key Identifier、authority Cert Issuer、authority Cert Serial Number）は、署名検証に用いる証明書発行者の鍵を識別する情報であり、鍵識別子、機関証明書発行者の名称、機関証明書シリアル番号を格納する。サブジェクト鍵識別子（subject key Identifier）は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。鍵使用目的（key usage）は、鍵の使用目的を指定するフィールドであり、（０）ディジタル署名用、（１）否認防止用、（２）鍵の暗号化用、（３）メッセージの暗号化用、（４）共通鍵配送用、（５）認証の署名確認用、（６）失効リストの署名確認用の各使用目的が設定される。秘密鍵有効期限(private Key Usage Period)は、証明書に格納した公開鍵に対応する秘密鍵の有効期限を記録する。認証局ポ

リシー（certificate Policies）は、公開鍵証明書発行者の証明書発行ポリシーを記録する。例えばＩＳＯ／ＩＥＣ９３８４－１に準拠したポリシーＩＤ、認証基準である。ポリシー・マッピング（policy Mapping）は、認証パス中のポリシー関係の制限に関する情報を格納するフィールドであり、認証局（ＣＡ）証明書にのみ必要となる。サブジェクト別名（subject Alt Name）は、証明書所有者の別名を記録するフィールドである。発行者別名（issuer Alt Name）は、証明書発行者の別名を記録するフィールドである。サブジェクト・ディレクトリ・アトリビュート（subject Directory Attribute）は、証明書所有者のために必要とされるディレクトリの属性を記録するフィールドである。基本制約（basic Constraint）は、証明対象の公開鍵が認証局（ＣＡ）の署名用か、証明書所有者のものかを区別するためのフィールドである。許容サブツリー制約名（name Constraints permitted Subtrees）は、発行者が発行する証明書の名前の制限情報を格納するフィールドである。制約ポリシー（policy Constraints）は、認証パス中のポリシーの関係の制限情報を格納するフィールドである。ＣＲＬ参照ポイント（Certificate Revocation List Distribution Points）は、証明書所有者が証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リストの参照ポイントを記述するフィールドである。署名アルゴリズム（Signature Algotithm）は、証明書の署名付けに用いるアルゴリズムを格納するフィールドである。署名は、公開鍵証明書発行者の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行者の秘密鍵を用いて生成したデータである。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【００４９】認証局は、図２～図４に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための失効リスト（Revocation List）の作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【００５０】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【００５１】（属性証明書（ＡＣ））属性証明書について図５を用いて説明する。属性証明書には大きく分けて２つの種類があり、１つは、コンテンツの利用権といった権利や権限に関する所有者の属性情報を含む証明書である。もう１つは、サービスプロバイダ（ＳＰ）用領域確保または削除用属性証明書（ＡＣ）であり、ユーザデバイス内のメモリにサービスプロバイダ（ＳＰ）用情報格納領域を確保または削除する場合の領域確保または削除の許諾情報を含む属性証明書（ＡＣ）である。

【００５２】属性証明書フォーマットはITU-T X.509で規定されており，IETF PKIX WGでProfileを策定している。公開鍵証明書とは異なり所有者の公開鍵を含まない。しかし属性証明書認証局(Attribute Certificate Authority)の署名がついているため、改竄されていないかどうかの判定はこの署名を検証することで行える、という点は公開鍵証明書と同様である。

【００５３】本発明の構成においては、属性証明書（ＡＣ）の発行管理を行なう属性証明書認証局(Attribute Certificate Authority)は、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２が兼務することが可能である。別の構成としてもよい。属性証明書は常に公開鍵証明書と関連づけて利用する。すなわち所有者の本人性自体は公開鍵証明書で確認し、その上で所有者にいかなる権限が与えられているかのみを示すものが属性証明書である。属性証明書の検証にあたっては，当該証明書の署名検証を行った後、それに関連づけられている公開鍵証明書の検証も行う。

【００５４】なお、その際、原則的には証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施することが好ましい。複数の認証局（ＣＡ）が存在し、階層構成をなす認証局構成では、下位の認証局自身の公開鍵証明書は、その公開鍵証明書を発行する上位認証局によって署名されている。すなわち、下層の公開鍵証明書発行局（ＣＡ－Ｌｏｗ）に対して上位の公開鍵証明書発行局（ＣＡ－Ｈｉｇｈ）が公開鍵証明書を発行するという連鎖的な公開鍵証明書発行構成をとる。公開鍵証明書の連鎖検証とは、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ルートＣＡ）までの公開鍵証明書の署名検証を行なうことを意味する。

【００５５】属性証明書の有効期間を短期間とすることにより、失効処理を行わないことも可能である。この場合、証明書の失効手続きや失効情報の参照手順等を省くことができ、システムが簡易となる長所がある。ただし証明書の不正利用に対しては失効以外の何らかの対策が必要となるため、十分に注意しなければならない。本認証システムにおいては、コンテンツに対する利用権限の他に、コンテンツを復号するためのコンテンツ鍵を属性証明書に埋め込んでおく構成であるので、正当なコンテンツ利用権限のあるユーザデバイスは、正当な属性証明書を受領することにより、コンテンツを利用可能である。

【００５６】図５に示す属性証明書の構成について説明する。証明書のバージョン番号は、証明書フォーマット

のバージョンを示す。ＡＣ保持者の公開鍵証明書情報、これは属性証明書（ＡＣ）の発行者に対応する公開鍵証明書（ＰＫＣ）に関する情報であり、ＰＫＣ発行者名、ＰＫＣシリアル番号、ＰＫＣ発行者固有識別子等の情報であり、対応公開鍵証明書を関連づけるリンクデータとしての機能を持つ。属性証明書の発行者の名前は、属性証明書の発行者、すなわち属性証明書認証局（ＡＡ）の名称が識別可能な形式（Distinquished Name）で記録されるフィールドである。署名アルゴリズム識別子は、属性証明書の署名アルゴリズム識別子を記録するフィールドである。証明書の有効期限は、証明書の有効期限である開始日時、終了日時が記録される。属性情報フィールドは、属性証明書の利用形態に応じて、（１）メモリ領域確保、削除情報、または、（２）コンテンツ利用条件関連情報のいずれかが格納される。コンテンツ利用条件関連情報には、暗号化されたコンテンツ鍵を含む。

【００５７】（１）メモリ領域確保、削除情報は、サービスプロバイダがユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ毎の管理領域を登録設定、または削除処理を目的として発行される属性証明書に記録される。記録情報は、例えば以下の情報である。

サービスプロバイダ識別子（ＩＤ）

サービスプロバイダ・ネーム

処理：メモリ領域確保、メモリ領域削除のいずれか

領域サイズ：メモリ領域のサイズ

【００５８】サービスプロバイダは、上記各項目を属性情報フィールドに格納した属性証明書をユーザデバイスに対して送付し、ユーザデバイスは属性証明書の検証の後、自己のセキュリティチップ内のメモリに、受信した属性証明書の属性情報フィールドの記録に従ったメモリ領域の確保処理、または確保済みのメモリ領域の削除処理を実行する。

【００５９】（２）コンテンツ利用条件関連情報は、サービスプロバイダの提供するコンテンツに対応して発行される属性証明書の属性情報フィールドに格納する情報であり、コンテンツの利用制限回数、利用期限等の様々な利用条件を含み、さらにコンテンツを暗号化したコンテンツ鍵の暗号化データを含む。記録情報は、例えば以下の情報である。

サービスプロバイダ識別子（ＩＤ）

サービスプロバイダ・ネーム

アプリケーション識別子（ＩＤ）：コンテンツの識別情報である。

条件：オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかを示す情報である。

有効期限：期間制限の場合の有効期限情報

利用制限回数：回数制限の場合の利用可能回数

支払条件：コンテンツの対価の支払条件を記録

コンテンツ鍵：暗号化されたコンテンツ鍵を暗号化アルゴリズム情報とともに格納

【００６０】コンテンツの利用態様には、上記条件フィールドに記載のように、（１）オンライン利用か、（２）オフライン利用かの区別と、（ａ）コンテンツを買い切りし、買い切り以後のコンテンツ利用をフリーとする態様、（ｂ）期間制限を設けてコンテンツの利用期間を設定した態様、（ｃ）回数制限を設けてコンテンツの利用回数を制限した態様の各態様がある。また期間制限と回数制限の両制限を伴うコンビネーション制限態様もある。ユーザデバイスでは、属性証明書に記録されたこれらの態様に従ってコンテンツの利用が実行される。これらの具体的な処理態様については、後段で説明する。

【００６１】また、暗号化コンテンツの復号鍵として適用するコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵が格納される。コンテンツ鍵：Ｋｃの暗号化処理に直接あるいは間接的に適用する鍵の主な種類は以下に示す通りである。

（ａ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ、（公開鍵方式）

（ｂ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵方式）

（ｃ）サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋ

（ｄ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇ

これらの鍵を適用した処理については後段で詳細に説明する。

【００６２】属性証明書には、さらに、署名アルゴリズムが記録され、属性証明書発行者である属性証明書認証局（ＡＡ）によって署名が施される。電子署名は、属性証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行者（ＡＡ）の秘密鍵を用いて生成したデータである。

【００６３】［セキュリティチップ構成］次にコンテンツを利用する情報処理装置としてのユーザデバイス内に構成されるセキュリティチップの構成について、図６を参照しながら説明する。なお、ユーザデバイスは、データ処理手段としてのＣＰＵ、通信機能を備えたＰＣ、ゲーム端末、ＤＶＤ，ＣＤ等の再生装置、記録再生装置等によって構成されるものであり、これらのユーザデバイスの中に耐タンパ構造を持つセキュリティチップが実装されることになる。ユーザデバイス自体の構成例は本明細書の末尾において説明する。セキュリティチップを持

つユーザデバイスは、図１におけるユーザデバイス製造者１０４において製造される。

【００６４】図６に示すように、ユーザデバイス２００には、セキュリティチップ２１０が、ユーザデバイス側制御部２２１に対して、相互にデータ転送可能な構成として内蔵される。セキュリティチップ２１０は、プログラム実行機能、演算処理機能を持つＣＰＵ（Central Processing Unit）２０１を有し、データ通信用のインタフェース機能を持つ通信インタフェース２０２、ＣＰＵ２０１によって実行される各種プログラム、例えば暗号処理プログラム、デバイスの製造時に格納されるマスター鍵：Ｋｍなどを記憶するＲＯＭ（Read Only Memory）２０３、実行プログラムのロード領域、また、各プログラム処理におけるワーク領域として機能するＲＡＭ（Random Access Memory）２０４、外部機器との認証処理、電子署名の生成、検証処理、格納データの暗号化、復号化処理等の暗号処理を実行する暗号処理部２０５、前述したサービスプロバイダ毎の情報、各種鍵データを含むデバイスの固有情報を格納した例えばＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)によって構成されるメモリ部２０６を有する。これら格納情報の詳細については後述する。

【００６５】ユーザデバイス２００は、暗号化コンテンツ等を格納する領域としてのＥＥＰＲＯＭ、ハードディスク等によって構成される外部メモリ部２２２を有する。外部メモリ部２２２は、公開鍵証明書、属性証明書の格納領域としても利用可能であり、また後段で説明するコンテンツの利用回数管理ファイルの格納領域としても利用される。

【００６６】セキュリティチップを搭載したユーザデバイスが、外部エンティテイ、例えばサービスプロバイダと接続し、データ転送処理を実行する場合には、必要に応じて、セキュリティチップ２１０と、外部エンティテイ間の相互認証が行われ、また転送データの暗号化が行なわれる。これらの処理の詳細については、後段で詳述する。

【００６７】ユーザデバイスのセキュリティチップでの処理対象となるデータ例を図７に示す。これらの多くは、不揮発性メモリの一形態であるフラッシュメモリ等のＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)によって構成されるメモリ部２０６に格納されるが、製造時に格納し、書き換え不可能とするデータ、例えばマスター鍵：Ｋｍは、ＲＯＭ（Read Only Memory）２０３に格納される。公開鍵証明書、属性証明書は、セキュリティチップ内のメモリに格納しても、外部メモリに格納してもよい。

【００６８】各データについて説明する。

公開鍵証明書（ＰＫＣ）：公開鍵証明書は、第三者に対して正当な公開鍵であることを示す証明書で、証明書には配布したい公開鍵を含み、信頼のおける認証局によりディジタル署名されている。ユーザデバイスには、前述した階層構成の最上位認証局（ルートＣＡ）の公開鍵証明書、ユーザデバイスに登録されたサービスプロバイダ、すなわち、ユーザデバイス内にメモリ領域が確保されているサービスプロバイダの公開鍵証明書、さらに、パスワード復帰処理等のサポートを実行するサポートセンタの公開鍵証明書を格納する。

【００６９】属性証明書（ＡＣ）：公開鍵証明書が証明書利用者（所有者）の“本人性”を示すのに対し、属性証明書は証明書利用者の利用権限を示すものである。利用者は属性証明書を提示することにより、属性証明書に記載された権利・権限に基づいて、アプリケーションの利用や、領域の確保などが行えるようになる。以下に、属性証明書の種類を示し、それぞれの果たす役割を示す。

【００７０】（ａ）アプリケーション利用管理用属性証明書（ＡＣ）：アプリケーションとは、一般に言われるコンテンツを広い意味で使用した表現であり、アプリケーションの種類としては、ゲーム、音楽、映画、金融情報等の各種アプリケーションがある。アプリケーション利用管理用属性証明書（ＡＣ）では、アプリケーションの利用権限に関しての記述があり、属性証明書（ＡＣ）をサービスプロバイダ（ＳＰ）に対して提示して検証、もしくは、ローカルで検証することにより、属性証明書（ＡＣ）に記述された利用権限範囲内でのアプリケーションの利用許諾が得られる。アプリケーションの利用権限に関する記述としては、アプリケーションのオンライン利用が可能であるかオフライン利用が可能であるか、さらに、オンライン利用可能なコンテンツの場合には、利用期間制限、利用回数制限情報があり、オフライン利用可能なコンテンツの場合には、利用回数制限、買い切りを示す記述がある。

【００７１】（ｂ）サービスプロバイダ（ＳＰ）用メモリ領域管理（確保）用属性証明書（ＡＣ）：ユーザデバイスにサービスプロバイダ（ＳＰ）を登録する場合、ＳＰに関する情報格納領域をユーザデバイス内に確保する必要がある。この時の領域確保の許諾情報を属性証明書（ＡＣ）に格納し、ユーザデバイスでは、属性証明書（ＡＣ）に格納された情報に従って、ユーザデバイス内にＳＰ用の領域を確保する。

【００７２】（ｃ）サービスプロバイダ（ＳＰ）用メモリ領域管理（削除）用属性証明書（ＡＣ）：ユーザデバイス内に確保したＳＰ用領域の削除の許諾情報を格納した属性証明書（ＡＣ）である。ユーザデバイスでは、属性証明書（ＡＣ）に格納された情報に従って、ユーザデバイス内のＳＰ用の領域の削除処理を実行する。

【００７３】鍵データ：鍵データとしては、デバイスに対して設定される公開鍵、秘密鍵のペア、コンテンツ等のデータ保存の際の暗号処理用鍵として用いられるストレージ鍵、さらに、乱数生成用鍵、相互認証用鍵等が格

納される。

【００７４】ストレージ鍵は、デバイスに保存するコンテンツ鍵の暗号化または復号化処理の少なくともいずれかに適用する鍵である。ストレージ鍵には、デバイス対応ストレージ鍵、サービスプロバイダ対応ストレージ鍵があり、サービスプロバイダ対応ストレージ鍵は、デバイスに登録された個々のサービスプロバイダ毎に各サービスプロバイダ管理領域内に格納される鍵であり、対応するサービスプロバイダの提供するコンテンツ鍵に対応して適用される。デバイス対応ストレージ鍵には、システムホルダと、デバイスのみが共有する鍵として構成されるグローバル共通鍵が含まれ、グローバル共通鍵は、サービスプロバイダにおける復号化処理を防止した暗号化コンテンツ鍵の配信処理を実行する際に用いられる。これらの鍵を適用した処理の詳細については後段で説明する。

【００７５】識別情報：識別情報としては、ユーザデバイス自身の識別子としてのデバイスＩＤ、ユーザデバイスに登録したサービスプロバイダ（ＳＰ）の識別子としてのサービスプロバイダＩＤ、ユーザデバイスを利用するユーザに付与されたユーザＩＤ、なお、ユーザＩＤはサービスプロバイダ等、外部エンティテイ毎に異なるユーザＩＤが付与可能である。アプリケーションＩＤは、サービスプロバイダ（ＳＰ）によって提供されるサービス、コンテンツに対応する識別情報としてのＩＤである。

【００７６】その他：ユーザデバイスには、さらに、認証情報として、ユーザデバイス内に登録したサービスプロバイダ（ＳＰ）情報の利用許諾を得るための認証情報（例えばパスワード）が格納される。パスワードを入力することにより、ユーザデバイス内に登録したサービスプロバイダ（ＳＰ）情報の取得が可能となり、情報取得後、サービスプロバイダの提供するアプリケーション、コンテンツの利用が許可される。認証情報（パスワード）を忘れた場合には、マスターパスワードを用いて認証情報（パスワード）の初期化（リセット）処理が可能である。

【００７７】さらに乱数生成用のシード情報が格納される。乱数は、認証処理、暗号処理等の際に、例えばＡＮＳＩ　Ｘ９．１７に従って生成する。

【００７８】さらに、コンテンツ利用回数情報、あるいはコンテンツ利用回数情報に基づいて算出されるハッシュ値が格納される。これは、アプリケーション、コンテンツに対応する属性証明書に格納された利用回数制限内でのコンテンツ利用を厳格に実行するために必要となる情報であり、コンテンツに対応する属性証明書の識別情報としてのアプリケーションＩＤ、属性証明書のシリアル番号、コンテンツの利用制限回数を保存する。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【００７９】［ユーザデバイス内のメモリ構成］不揮発性メモリの一形態であるフラッシュメモリ等のＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)によって構成されるメモリ部２０６には、上述した様々なデータの少なくとも一部が格納されるが、これらは、メモリ部２０６領域に分割管理された３つの領域、すなわち、（１）デバイス管理領域、（２）システム管理領域、（３）サービス・プロバイダ管理領域に区分されて格納される。以下、これらの各領域毎の格納データについて説明する。

【００８０】（１）デバイス管理領域

デバイス管理領域は、デバイス固有のシステムに依存しない情報が保持されている。この領域はデバイス製造時に、最初に領域が確保され、不揮発性メモリの先頭の複数ブロックを占める領域である。デバイス管理領域では、少なくとも以下のデータを保持・管理する。

デバイスＩＤ

乱数生成用シード

乱数生成用暗号鍵

相互認証鍵

デバイス対応ストレージ鍵

【００８１】相互認証鍵は、セキュリティチップ内のデータをセキュリティチップ外部に出力する場合等に出力先となるエンティテイとの認証用の鍵である。なお、エンティテイは、セキュリティチップを装着した例えばゲーム端末、ＤＶＤ，ＣＤ等の再生装置、記録再生装置であるユーザデバイスも含む。セキュリティチップと、セキュリティチップを持つユーザデバイス間でのデータ転送、さらにはユーザデバイスを介した外部のサービスプロバイダとのデータ通信時などに相互認証鍵を適用した相互認証処理が実行される。相互認証の成立を条件として、相互認証時に生成したセッション鍵で暗号化してセキュリティチップ内部と外部間のデータ転送が実行される。

【００８２】デバイス対応ストレージ鍵は、セキュリティチップ内部のデータを外部に保持する場合に、データを暗号化し、閲覧・改竄を防ぐための鍵である。デバイス・ストレージ鍵は、公開鍵系でも共通鍵系でもどちらでもよい。乱数生成用シードは、擬似乱数を算術演算により求める際に、初期シードとして用いるデータである。乱数生成用暗号鍵を用いて擬似乱数を算術演算して乱数を生成する。

【００８３】共通鍵系デバイス対応ストレージ鍵には、システムホルダと、デバイスのみが共有する鍵として構成されるグローバル共通鍵が含まれ、グローバル共通鍵は、サービスプロバイダにおける復号化処理を防止した暗号化コンテンツ鍵の配信処理を実行する際に用いられる。グローバル共通鍵については、後段で詳細に説明する。

【００８４】（２）システム管理領域
システム管理領域は、デバイス管理領域と同様にメモリ領域に確保される。システム管理領域では、以下のデータを保持・管理する。
ルート認証局（ＣＡ）公開鍵証明書
デバイス公開鍵証明書
デバイス秘密鍵
【００８５】ルート認証局（ＣＡ）公開鍵証明書は、セキュリティチップ内の認証系すべての根源となる証明書で、他の証明書の署名検証を辿って、前述の連鎖検証を行なうと、最後にはルート認証局（ＣＡ）の公開鍵証明書に辿り着くことになる。
【００８６】デバイス公開鍵証明書は、サービスプロバイダとの相互認証時に用いる公開鍵証明書である。デバイス秘密鍵を外部で生成し、インポートする場合には、デバイス公開鍵証明書も同時に生成される。デバイス側でデバイス秘密鍵・公開鍵を生成する場合には、デバイス内でデバイス秘密鍵・公開鍵が生成された後に、デバイス公開鍵がデバイスから読み出され、デバイス公開鍵証明書の発行処理を行ない、発行されたデバイス公開鍵証明書のインポートが行われる。
【００８７】デバイス秘密鍵は、データに対して署名付けおよび認証するための鍵である。秘密鍵は、公開鍵とペアで生成されるが、予め外部で生成して、デバイスにセキュアにインポートする構成とするか、デバイス内部で生成し、決して外部に出さない構成とするかのいずれかの構成とする。
【００８８】（３）サービスプロバイダ管理領域
サービスプロバイダ（ＳＰ）管理領域は、サービスプロバイダ（ＳＰ）管理テーブルとサービスプロバイダ（ＳＰ）管理情報とからなる。サービスプロバイダ（ＳＰ）管理テーブルは、サービスプロバイダ（ＳＰ）管理領域内で各サービスプロバイダ（ＳＰ）情報の所在を示すためのテーブルでありサービスプロバイダの識別子に対応させてメモリの各サービスプロバイダ（ＳＰ）情報の格納位置情報を持つ。
【００８９】なお、サービスプロバイダ（ＳＰ）管理領域には、ユーザデバイスがサービスプロバイダ（ＳＰ）毎に会員登録を行うことにより、サービスプロバイダ（ＳＰ）毎の領域がデバイス内のメモリ領域に確保される。なお、領域確保あるいは削除処理は、属性証明書の記述に基づいて実行される。サービスプロバイダ（ＳＰ）管理領域には、以下の情報を保持する。
【００９０】サービスプロバイダ（ＳＰ）対応秘密鍵
サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵（公開鍵方式）
サービスプロバイダ（ＳＰ）対応ストレージ鍵（共通鍵方式）
外部管理情報のハッシュ値
コンテンツ利用回数管理データ
認証情報
ユーザ情報
【００９１】サービスプロバイダ（ＳＰ）対応秘密鍵は、登録サービスプロバイダ（ＳＰ）毎に対応して生成した登録サービスプロバイダ（ＳＰ）との相互認証処理または暗号化データ転送処理等に適用する公開鍵と秘密鍵のペアの秘密鍵である。登録サービスプロバイダ（ＳＰ）と、セキュリティチップとが相互認証する場合に必要とする鍵である。
【００９２】サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵（公開鍵方式）は、サービスプロバイダの提供するコンテンツ利用をオフラインで利用可能である場合、すなわち、取得したコンテンツを利用する毎にサービスプロバイダとの接続を必要としないコンテンツである場合、コンテンツに対応する暗号化コンテンツ鍵の復号用の鍵である。暗号化コンテンツ鍵は、サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵によってサービスプロバイダにおいて暗号化されて属性証明書（ＡＣ）に格納されてユーザデバイスに送信され、ユーザデバイスのセキュリティチップ内でサービスプロバイダ（ＳＰ）対応ストレージ秘密鍵で復号してコンテンツ鍵の取得が可能となる。
【００９３】サービスプロバイダ（ＳＰ）対応ストレージ鍵（共通鍵方式）は、サービスプロバイダの提供するコンテンツ利用をオフラインで利用可能である場合、すなわち、取得したコンテンツを利用する毎にサービスプロバイダとの接続を必要としないコンテンツである場合、コンテンツに対応する暗号化コンテンツ鍵の復号用の鍵であり、暗号化、復号化処理に共通に適用可能な鍵である。なお、サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵（公開鍵方式）と、サービスプロバイダ（ＳＰ）対応ストレージ鍵（共通鍵方式）は、いずれか一方のみを格納し適用する構成としてもよい。。
【００９４】外部管理情報のハッシュ（Ｈａｓｈ）値は、セキュリティチップ内部で管理するには大きすぎるデータを外部メモリの特定領域に出し、その領域のハッシュ値をセキュリティチップ内で管理することにより、改竄ができないようにするものである。例えば、コンテンツの回数利用制限をかける場合に、残回数などがハッシュ値による管理対象となる。回数管理コンテンツの場合、回数情報の閲覧自体は問題ないが、改竄は防がなくてはならない。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。
【００９５】コンテンツ利用回数管理データ
アプリケーション（コンテンツ）の利用可能回数をセキュリティチップがローカルで管理する場合がある。この時、セキュリティチップ内部では、アプリケーションＩＤ、属性証明書（ＡＣ）のシリアル、利用可能回数とを

保持・管理する。コンテンツ利用回数管理データの管理処理については、後段で詳細に説明する。

【００９６】認証情報

認証情報とは、サービスプロバイダ（ＳＰ）管理領域で管理される管理情報を保護する目的の情報である。ユーザはサービスプロバイダ（ＳＰ）接続時にはサービスプロバイダ（ＳＰ）との相互認証が必要となるが、相互認証に必要な情報は、サービスプロバイダ（ＳＰ）管理領域に格納される。この管理領域から必要情報を取得するために用いるのが認証情報である。認証情報は具体的には、例えばパスワードである。認証情報（パスワード）をユーザが忘れた場合には、サービスプロバイダ（ＳＰ）管理領域の管理情報の利用許諾が得られなくなる。この場合には、マスター・パスワードを入力することにより認証情報自体のリセット、または変更を行うことができる。これらの処理構成については、後段で詳細に説明する。

【００９７】ユーザ情報

ユーザ情報は、サービスプロバイダ（ＳＰ）により割り振られたユーザＩＤなどのユーザ固有情報である。

【００９８】［パスワード管理］以下、図１に示すユーザデバイス１０１が、サービスプロバイダ（コンテンツディストリビュータ）１０２の提供するコンテンツを受領し、属性証明書に従った利用制限の下にコンテンツを利用する処理、およびコンテンツ利用に際して必要となる各種処理の詳細について説明する。まず、コンテンツを提供するサービスプロバイダに関する情報を格納したユーザデバイス内のメモリ領域のサービスプロバイダ管理領域へのアクセス制御用の認証情報（パスワード）について説明する。

【００９９】（１）認証情報（パスワード）登録処理

ユーザデバイスを購入したユーザがシステムホルダの管理下にある様々なサービスプロバイダからコンテンツを購入する処理、あるいは購入したコンテンツを利用する処理を行なうためには、ユーザデバイス内のメモリ領域にサービスプロバイダ管理領域を設定し、このサービスプロバイダ管理領域にサービスプロバイダ毎の管理情報を格納する処理が必要となる。ユーザデバイス内のメモリ領域にサービスプロバイダ管理領域の設定されたサービスプロバイダを、以下登録サービスプロバイダと呼ぶ。サービスプロバイダ管理領域の設定には、前述の属性証明書を適用し、ユーザデバイスがサービスプロバイダから受信した属性証明書に基づいて、ユーザデバイス内のメモリ領域に属性証明書の記録に従ったサービスプロバイダ管理領域の設定処理を実行する。

【０１００】サービスプロバイダ管理領域を持つ登録サービスプロバイダに対して、ユーザデバイスがアクセスしてコンテンツの購入、あるいは利用を行なうためには、先ず、ユーザデバイス内のサービスプロバイダ管理領域内の情報を取得することが必要となる。サービスプロバイダ管理領域には、ユーザデバイスとサービスプロバイダ間の相互認証処理に必要な情報が格納されており、これらの情報を取得してサービスプロバイダとの相互認証を行なうことが必要となるからである。

【０１０１】このサービスプロバイダ管理領域にアクセスするためにユーザは各登録サービスプロバイダ毎に設定される認証情報(パスワード)を、ユーザデバイスの入力手段を介して入力することが必要となる。なお、以下の説明において、「サービスプロバイダ毎に」との記述は、「各登録サービス毎かつ各ユーザ毎」と同義である。セキュリティチップ側で入力パスワードと登録パスワードの一致検証を行ない、一致した場合に限り、セキュリティチップ内のメモリに形成されたサービスプロバイダ管理領域内の情報取得が可能となり、その後のサービスプロバイダとの相互認証処理、へのアクセスが可能となる。

【０１０２】認証情報（パスワード）は、ユーザデバイスに登録されたサービスプロバイダ毎に設定される。これらのパスワードの初期登録は、ユーザ自身が実行する。パスワードの初期登録処理について、図８を参照して説明する。図８のシーケンス図において、左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスにおけるユーザインタフェース側処理である。

【０１０３】まず、（１）パスワード登録対象となる対応するサービスプロバイダを指定して認証情報（パスワード）初期登録処理開始要求をユーザが入力する。

（２）セキュリティチップ側では、ユーザの指定したサービスプロバイダが、セキュリティチップ内のメモリにすでに管理領域を設定済みの登録サービスプロバイダであり、パスワード設定されていない状態であるか等のステータス確認処理を行ない、これらが確認された場合に、（３）認証情報（パスワード）初期登録処理を許可する。

【０１０４】次に、ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（４）パスワードを入力し、（５）セキュリティチップの制御部は入力された認証情報（パスワード）をテンポラリにメモリに保持し、（６）同一パスワードの再入力要求を行ない、

（７）ユーザにより認証情報（パスワード）の再入力がなされると、（８）セキュリティチップの制御部は再入力認証情報（パスワード）とテンポラリにメモリに保持してある認証情報（パスワード）の照合を実行し、照合が成立した場合には、（９）認証情報（パスワード）の書き込み処理を実行し、（１０）書き込み結果をユーザに通知し、ＯＫなら終了する。（１１）ＮＧの場合は、（１）の処理に戻る。

【０１０５】（２）認証情報（パスワード）変更処理

図９および図１０にパスワードの変更処理のシーケンス図を示す。パスワード変更は、登録済みパスワードを用

いた変更処理（通常時）と、マスターパスワードを用いた変更処理（緊急時）の２つの処理態様がある。

【０１０６】まず、図９のシーケンス図に基づいて、通常時のパスワード変更処理、すなわち、登録済みパスワードを用いた変更処理について説明する。左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスのユーザインタフェース側処理である。

【０１０７】まず、（１）パスワード変更処理対象となる対応するサービスプロバイダを指定して認証情報（パスワード）変更処理開始要求をユーザが入力する。

（２）セキュリティチップ側では、ユーザの指定したサービスプロバイダがメモリに管理領域を設定され登録済みのサービスプロバイダ（ＳＰ）であり、パスワードの設定されたＳＰであるか等のステータス確認を処理を行ない、これらが確認されたことを条件として、（３）登録済みの認証情報（パスワード）入力要求を行なう。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（４）登録済みパスワードを入力し、

（５）セキュリティチップの制御部は入力を確認すると、サービスプロバイダ管理領域に書き込まれている登録認証情報（パスワード）との照合処理を実行する。

【０１０８】照合が成立すると、（６）変更処理許可を通知する。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（７）新たな認証情報（パスワード）を入力し、（８）セキュリティチップの制御部は入力された認証情報（パスワード）をテンポラリにメモリに保持し、（９）同一パスワードの再入力要求を行ない、（１０）ユーザにより認証情報（パスワード）の再入力がなされると、（１１）セキュリティチップの制御部は再入力認証情報（パスワード）とテンポラリにメモリに保持してある認証情報（パスワード）の照合を実行し、照合が成立した場合には、（１２）認証情報（パスワード）の書き込み処理を実行し、（１３）書き込み結果をユーザに通知し、ＯＫなら終了する。（１４）ＮＧの場合は、（１）の処理に戻る。

【０１０９】（３）マスターパスワードを用いた認証情報（パスワード）リセット処理

次に、図１０のシーケンス図に基づいて、緊急時のパスワード変更処理等において実行されるマスターパスワードを用いた認証情報（パスワード）リセット処理について説明する。左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスを装着した端末におけるユーザインタフェース側処理である。

【０１１０】まず、（１）パスワード変更処理対象となる対応するサービスプロバイダを指定して認証情報（パスワード）リセット処理開始要求をユーザが入力する。

（２）セキュリティチップ側では、ユーザの指定したサービスプロバイダがメモリに管理領域を設定され登録済みのサービスプロバイダ（ＳＰ）であり、パスワードの設定されたＳＰであるか等のステータス確認を処理を行ない、これらの条件を満足する場合に、（３）マスターパスワード入力要求を行なう。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（４）マスターパスワードを入力し、（５）セキュリティチップの制御部は入力されたマスターパスワードの照合処理を実行し、正しいマスターパスワードの入力であるか否かを判定し、検証の結果、正しいマスターパスワード入力であると判定すると、（６）サービスプロバイダ管理領域に書き込まれている登録認証情報（パスワード）の初期化、すなわち登録済み認証情報（パスワード）のリセット処理を実行する。

【０１１１】セキュリティチップの制御部は、リセット処理の後、（７）処理結果通知をユーザに通知し、ＯＫであれば、例えば、ユーザは前述の認証情報（パスワード）登録処理を実行する。これらの処理は、先に図８を参照して説明した処理と同様であるので説明を省略する。（８）リセット処理結果がＮＧの場合は、（１）の処理に戻る。

【０１１２】図１０の処理シーケンスを用いて説明したように、マスターパスワードは、各登録サービスプロバイダについて登録済みの認証情報(パスワード)の初期化処理、すなわちリセットする際に適用される。マスターパスワードを用いた認証情報初期化（リセット）処理は、セキュリティチップに登録されたサービスプロバイダすべての認証情報に対して有効である。

【０１１３】図１１にマスターパスワードと各登録サービスプロバイダの認証情報（パスワード）との関係図を示す。図１１に示すようにマスターパスワードは、各サービスプロバイダ対応認証情報に対する上位パスワードとして存在し、マスターパスワードの入力により、各各登録サービスプロバイダの認証情報（パスワード）の初期化（リセット）が実行され、新たな認証情報を各登録サービスプロバイダの認証情報（パスワード）として再登録することが可能となる。

【０１１４】マスターパスワードは、図１２に示すように、ユーザデバイスの購入時に例えばプリントされた用紙がデバイスに添付されて配布される。マスターパスワードはデバイスの製造時に工場で書き込まれるが、ユーザによるマスターパスワードのデバイスからの読み出しはできない構成となっている。マスターパスワードは、デバイスに固有の識別子であるデバイスＩＤと、マスターキーに基づいて生成される。マスターキーは情報処理装置個々または一群の情報処理装置に対応して設定されるキーである。

【０１１５】マスターパスワードをユーザが忘れた場合には、サポートセンターへの登録を条件としてマスターパスワードの再発行処理が可能となる。図１３にサポートセンタへのユーザ登録処理および、マスターパスワードの再発行処理シーケンス図を示す。

【０１１６】図１３の上段が、サポートセンタに対する

ユーザ登録処理シーケンス図を示す。ユーザは購入デバイスに添付された登録用紙の郵送、あるいはデバイスを設定した端末を介してサポートセンタに接続してユーザ登録を行なうことができる。ユーザ登録は、ユーザ住所、電話番号、デバイスのＩＤ等のデータをサポートセンタに登録する処理として実行され、サポートセンタにおいてユーザ登録が完了すると、ユーザ登録完了通知がサポートセンタからユーザに送付または送信される。

【０１１７】図１３の下段が、ユーザがマスターパスワードを忘れた場合に、ユーザと、サポートセンタ間で実行されるマスターパスワード再発行処理のシーケンスである。ユーザは、デバイスＩＤを伴うユーザ情報データとともに、マスターパスワードの再発行要求をサポートセンタに対して送信し、サポートセンタが要求を受信すると、サポートセンタは、ユーザ情報、ユーザＩＤが登録済みデータと一致するかを判定し、一致した場合は、ユーザデバイスＩＤに基づくマスターパスワードの検索あるいはマスターキーを用いたマスターパスワードの生成処理を実行する。サポートセンタは、情報処理装置としてのユーザデバイスに対応して設定されたデバイス識別子としてのデバイスＩＤと、マスターパスワードとを対応させたマスターパスワード格納データベースを有する。あるいは、デバイスＩＤと、デバイス個々に固有のキー、または一群のデバイスに共通するキーとして設定されたマスターキーとを対応させたマスターキー格納データベースのいずれかを有し、マスターパスワード格納データベースを有する場合には、デバイスＩＤに基づいてデータベース検索を実行してマスターパスワードを取得する。マスターキー格納データベースを有する場合には、デバイスＩＤに対する、マスターキーを適用した暗号処理によるマスターパスワード生成処理を実行し、生成したマスターパスワードをユーザデバイスに送付する処理を実行する。

【０１１８】ユーザデバイスＩＤに基づくマスターキーによるマスターパスワードの生成処理フローを図１４に示す。図１４のフローについて説明する。まず、ステップＳ１０１において、マスターキーＫｍ１を用いてデバイスＩＤの暗号化処理を実行する。その結果をステップＳ１０２において、ＭＰａとする。さらに、結果ＭＰａに対してマスタキーＫｍ２を適用した暗号化処理を実行してパスワードＭＰを得て、ステップＳ１０３において、ＡＳＣＩＩコードに変換する。暗号化処理は例えばＤＥＳ，トリプルＤＥＳ等の暗号化アルゴリズムが適用可能である。マスターキーＫｍ１，Ｋｍ２は、複数のデバイスに対して共通に設定されたキーであり、サポートセンタはユーザデバイスＩＤに基づいて、サポートセンタで保持する複数のキーから適用すべきマスターキーを選択して使用する。

【０１１９】図１３のシーケンス図に戻って説明を続ける。サポートセンタでマスターパスワードの生成が実行されると、サポートセンタは、マスターパスワードをオンラインまたはオフラインでユーザまたはユーザデバイスに対して送信または送付する。

【０１２０】以上のシーケンスに従って、ユーザは、サポートセンタを利用してマスターパスワードの再発行処理を行なうことができる。なお、ユーザデバイスと、サポートセンタ間においては、データ送受信の前処理として相互認証処理を実行し、送受信する秘密データ、例えばユーザＩＤ、マスターパスワード等は相互認証時に生成したセッションキーで暗号化し、またデータの改竄防止のために署名の生成、検証を行なうことが好ましい。なお、これら相互認証処理、署名生成、検証処理等の詳細については、コンテンツの配信処理の項目で詳しく説明する。

【０１２１】また、ユーザは、サポートセンタを利用したマスターパスワードの再発行処理をオフラインで行なうことも可能である。この場合は、ハガキなどに本人確認のための情報を記入して送付するなどの処理が行なわれることになる。

【０１２２】［コンテンツ配信処理］ユーザデバイス内のセキュリティチップ内のメモリ領域にサービスプロバイダの管理領域が登録され、サービスプロバイダとの認証に必要な情報、上記パスワード等が登録されると、これらの情報を用いてサービスプロバイダとの通信によるコンテンツ購入が可能となる。以下、コンテンツ購入処理の詳細について説明する。

【０１２３】コンテンツ購入処理における概要を説明するシーケンス図を図１５に示す。左側がセキュリティチップを持つユーザデバイス側処理であり、右側がサービスプロバイダ側処理である。

【０１２４】ユーザデバイスは、まず、コンテンツの購入要求をサービスプロバイダに出力する。サービスプロバイダがコンテンツ購入要求を受信すると、ユーザデバイスとサービスプロバイダ間において相互認証が実行される。相互認証が成立し、双方の正当性が確認されると、サービスプロバイダは、購入要求コンテンツに対応する属性証明書（ＡＣ:Attribute Certificate）を生成し、ユーザデバイスに送信する。属性証明書には、コンテンツを復号するためのコンテンツ鍵：Ｋｃが暗号化されて格納され、また、利用回数、利用期限等のコンテンツ利用条件が記録されている。また格納データに対して属性証明書発行者である属性証明書認証局（ＡＡ:Attribute Certificate Authority）の署名がなされており、改竄防止を考慮したものとなっている。

【０１２５】属性証明書を受信したユーザデバイスは、属性証明書の署名検証処理を実行し、改竄なしの判定に基づいて属性証明書をメモリに保存する。さらに、ユーザデバイスは、コンテンツの要求をサービスプロバイダに対して行ない、サービスプロバイダは、先にユーザデバイスに送付した属性証明書内に格納されたコンテンツ

鍵：Ｋｃで暗号化したコンテンツをユーザデバイスに送付する。ユーザデバイス側では、属性証明書から取り出した暗号化されたコンテンツ鍵の復号化処理を実行してコンテンツ鍵を取り出し、取り出したコンテンツ鍵を適用した暗号化コンテンツの復号化処理によりコンテンツを取得し、利用する。なお、属性証明書に格納したコンテンツ鍵の復号化処理をサービスプロバイダ側で実行する態様（オンライン復号）もある。これらの具体的処理例については、後段で説明する。

【０１２６】コンテンツ配信に伴う大まかな流れは、以上、図１５を用いて説明した通りである。以下、各処理の詳細について説明する。なお、図１５に示した処理シーケンスでは、コンテンツに対応する属性証明書を暗号化コンテンツ送付の先に実行しているが、暗号化コンテンツの配信と、属性証明書の配信はいずれが先でもよく、同時に配信する処理としてもよい。また、それぞれをディスク等の記録媒体に格納して配信するオフライン配信を行なう構成とすることも可能である。

【０１２７】また、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０１２８】（１）相互認証処理、

コンテンツの購入要求エンティテイであるユーザデバイス、およびコンテンツの提供元であるサービスプロバイダ間では、まず相互認証処理が実行される。データ送受信を実行する２つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。相互認証方式としては、公開鍵暗号方式、共通鍵暗号方式等、各方式の適用が可能である。

【０１２９】ここでは、公開鍵暗号方式の１つの認証処理方式であるハンドシェイクプロトコル（ＴＬＳ１．０）について図１６のシーケンス図を参照して説明する。

【０１３０】図１６において、左側がユーザデバイス(クライアント)の処理、右側がサービスプロバイダ（サーバ）側の処理を示している。まず、（１）サービスプロバイダ（サーバ）が暗号化仕様を決定するためのネゴシエーション開始要求をハローリクエストとしてユーザデバイス（クライアント）に送信する。（２）ユーザデバイス（クライアント）はハローリクエストを受信すると、利用する暗号化アルゴリズム、セッションＩＤ、プロトコルバージョンの候補をクライアントハローとして、サービスプロバイダ（サーバ）側に送信する。

【０１３１】（３）サービスプロバイダ（サーバ）側は、利用を決定した暗号化アルゴリズム、セッションＩＤ、プロトコルバージョンをサーバーハローとしてユーザデバイス（クライアント）に送信する。（４）サービスプロバイダ（サーバ）は、自己の所有するルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式をユーザデバイス（クライアント）に送信（サーバ・サーティフィケート）する。なお、証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施しない場合には、必ずしもルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式を送付する必要はない。（５）サービスプロバイダ（サーバ）は、ＲＳＡ公開鍵またはＤｉｆｆｉｅ＆Ｈｅｌｌｍａｎ公開鍵情報をユーザデバイス（クライアント）に送信（サーバ・キー・エクスチェンジ）する。これは証明書が利用できない場合に一時的に適用する公開鍵情報である。

【０１３２】（６）次にサービスプロバイダ（サーバ）側は、ユーザデバイス（クライアント）に対してサーティフィケート・リクエストとして、ユーザデバイス（クライアント）の有する証明書を要求し、（７）サービスプロバイダ（サーバ）によるネゴシエーション処理の終了を知らせる（サーバハロー終了）。

【０１３３】（８）サーバハロー終了を受信したユーザデバイス（クライアント）は、自己の所有するルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式をサービスプロバイダ（サーバ）に送信（クライアント・サーティフィケート）する。なお、公開鍵証明書の連鎖検証を行なわない場合は公開鍵証明書の一式送付は必須ではない。（９）ユーザデバイス（クライアント）は、４８バイト乱数をサービスプロバイダ（サーバ）の公開鍵で暗号化してサービスプロバイダ（サーバ）に送信する。サービスプロバイダ（サーバ）、ユーザデバイス（クライアント）は、この値をもとに送受信データ検証処理のためのメッセージ認証コード：ＭＡＣ（Message Authentication Code）生成用のデータ等を含むマスターシークレットを生成する。

【０１３４】（１０）ユーザデバイス（クライアント）は、クライアント証明書の正しさを確認するため、ここまでのメッセージのダイジェストをクライアントの秘密鍵で暗号化してサービスプロバイダ（サーバ）に送信（クライアントサーティフィケート確認）し、（１１）先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（１２）認証の終了を通知する。一方、（１３）サービスプロバイダ

（サーバ）側からユーザデバイス（クライアント）に対しても、先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（１４）認証の終了を通知する。

【０１３５】上記処理において決定された暗号化アルゴリズムに従ってユーザデバイス（クライアント）とサービスプロバイダ（サーバ）間のデータ転送が実行されることになる。

【０１３６】データ改竄の検証は、上述の認証処理でユーザデバイス（クライアント）とサービスプロバイダ（サーバ）間の合意のもとに生成されたマスターシークレットから算出されるメッセージ認証コード：ＭＡＣ（Message Authentication Code）を各エンティティの送信データに付加することでメッセージの改竄検証を行なう。

【０１３７】図１７にメッセージ認証コード：ＭＡＣ（Message Authentication Code）の生成構成を示す。データ送信側は、送信データに対して、認証処理において生成したマスターシークレットに基づいて生成されるＭＡＣシークレットを付加し、これらの全体データからハッシュ値を計算し、さらにＭＡＣシークレット、パディング、ハッシュ値に基づいてハッシュ算出を行なってメッセージ認証コード（ＭＡＣ）を生成する。この生成したＭＡＣを送信データに付加して、受信側で受信データに基づいて生成したＭＡＣと受信ＭＡＣとの一致が認められればデータ改竄なしと判定し、一致が認められない場合には、データの改竄があったものと判定する。

【０１３８】（２）コンテンツ利用権限情報証明書（属性証明書）の生成、送信

ユーザデバイスからコンテンツの要求がなされたサービスプロバイダは、要求コンテンツの復号化処理に適用可能なコンテンツ鍵：Ｋｃを暗号化して格納し、コンテンツの利用制限情報を格納したコンテンツ利用権限情報証明書、例えば属性証明書（ＡＣ）を生成して、ユーザに対して送信する。

【０１３９】コンテンツ利用権限情報証明書、例えば属性証明書（ＡＣ）を生成する主体は、サービスプロバイダ自身であっても、またコンテンツ管理を実行する外部エンティティであってもよい。外部エンティティが属性証明書（ＡＣ）を生成する場合は、サービスプロバイダの要求に従ってその外部エンティティが属性証明書（ＡＣ）を生成する。

【０１４０】属性証明書には対応暗号化コンテンツの復号に適用可能なコンテンツ鍵：Ｋｃが暗号化されて格納される。コンテンツ鍵Ｋｃの暗号化に適用する鍵には、例えば、

（ａ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ

（ｂ）サービスプロバイダの保有する秘密鍵（共通鍵系）：ＳＰ．Ｓｔｏ．Ｋ

（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇ

の各態様がある。なお、この他にも、いくつかの態様が可能である。例えばサービスプロバイダの保有する公開鍵で暗号化することも可能である。この場合は、ユーザデバイスから属性証明書（ＡＣ）を受信してサービスプロバイダの保有する秘密鍵で復号化することになる。

【０１４１】なお、いずれの暗号化態様を適用した場合でも、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。以下、上記（ａ）～（ｃ）の態様における処理の詳細について説明する。

【０１４２】（ａ）ＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを適用した場合

前述したユーザデバイスのセキュリティチップのメモリ領域についての説明中で示したように、ユーザデバイスに登録された各登録サービスプロバイダについては、メモリに形成された各サービスプロバイダ管理領域にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋが格納される。ユーザデバイスのセキュリティチップでは、サービスプロバイダから提供されるコンテンツに対応する属性証明書の中からＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋで暗号化されたコンテンツ鍵：Ｋｃ、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、ＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋで復号化処理を実行することにより、コンテンツ鍵：Ｋｃを取得する。なお、［Ａ（Ｂ）］は、Ａで暗号化されたＢからなるデータを示すものとする。本形態では、ユーザデバイスは、コンテンツの利用時、すなわち復号時にサービスプロバイダと接続することなくユーザデバイス内の処理としてコンテンツ復号、すなわちオフライン復号が可能となる。

【０１４３】なお、上記例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成例について説明したが、共

33

通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋを用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納する。

【０１４４】（ｂ）サービスプロバイダの保有する秘密鍵（共通鍵系）：ＳＰ．Ｓｔｏ．Ｋを適用した場合

サービスプロバイダは、ユーザデバイスに対して提供するコンテンツに対応して設定される属性証明書に格納するコンテンツ鍵：Ｋｃをサービスプロバイダが保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを適用して暗号化する。ユーザデバイスは、属性証明書を受信しても、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］を復号することはできない。サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋはユーザデバイスは保有していないからである。

【０１４５】従って、コンテンツを利用（復号化）するためには、次のような処理が必要となる。まず、ユーザデバイスは、サービスプロバイダに属性証明書を送付してコンテンツ鍵の復号要求を行ない、サービスプロバイダにおいては、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋによってコンテンツ鍵：Ｋｃの復号化を行なう。ユーザデバイスはサービスプロバイダより復号化されたコンテンツ鍵：Ｋｃを取得し、該コンテンツ鍵：Ｋｃで暗号化コンテンツの復号を行なう。本形態では、上述の（ａ）の形態と異なり、ユーザデバイスは、コンテンツの利用時、すなわち復号時にサービスプロバイダと接続することが必須となる。すなわちオンライン処理が必要となる。

【０１４６】（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇを適用した場合

このグローバル共通鍵を利用する形態は、コンテンツの配信を実行するサービスプロバイダにおいて、システムホルダの許可なくコンテンツが配布、利用されることを防止し、システムホルダ（ＳＨ）による管理されたコンテンツ配信を行なうための構成である。サービスプロバイダに対してコンテンツを提供するコンテンツクリエータの有するコンテンツ製作者鍵、コンテンツ配信を行なうサービスプロバイダの有するコンテンツ配信者鍵、そしてシステムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇの各鍵を組み合わせた暗号化処理を行なった暗号化鍵データを属性証明書に格納し、コンテンツ利用者としてのエンドエンティティであるユーザデバイスに配布することで、サービスプロバイダ自体もコンテンツ鍵を取り出すことを防止し、ユーザデバイスにおいてのみコンテンツ鍵：Ｋｃを取り出すことを可能とした構成である。

34

【０１４７】以下、これらの各形態について詳細に説明する。まず、上記（ａ）～（ｃ）に共通する属性証明書の発行処理シーケンスについて図１８を用いて説明する。

【０１４８】図１８の処理シーケンスは、先に説明した図１５のコンテンツ購入処理シーケンスの一部として構成される属性証明書の生成、送信処理を詳細に説明したものである。ユーザデバイスはセキュリティチップを内蔵し、セキュリティチップ内のメモリにはサービスプロバイダ管理領域が生成されており、サービスプロバイダ管理情報が格納済みであるとする。

【０１４９】図１８の処理について説明する。ユーザデバイスとサービスプロバイダ間の相互認証が成立後、

（１）セキュリティチップを持つユーザデバイスは、サービスプロバイダに対して属性証明書（ＡＣ）の要求を行なう。属性証明書（ＡＣ）要求には、サービスプロバイダ管理領域に登録されたユーザＩＤ、コンテンツの指定識別子としてのアプリケーションＩＤ、さらにユーザが選択した利用条件データにユーザの秘密鍵（サービスプロバイダ対応秘密鍵）で署名したデータにユーザの公開鍵証明書（ＰＫＣ）を添付して送信する。利用条件データは、例えばコンテンツ利用制限回数、利用期限等の指定データであり、ユーザによって選択可能である場合にユーザ指定データとして含まれる。

【０１５０】署名は、データ改竄の検証を可能とするために付加されるものであり、前述のＭＡＣ値を用いることも可能であり、公開鍵暗号方式を用いた電子署名を適用することも可能である。

【０１５１】公開鍵暗号方式を用いた電子署名の生成方法について、図１９を用いて説明する。図１９に示す処理は、ＥＣ－ＤＳＡ（（Elliptic Curve Digital SignatureAlgorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptosystem（以下、ＥＣＣと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【０１５２】図１９の各ステップについて説明する。ステップＳ１において、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$y^2 = x^3 + ax + b$，$4a^3 + 27b^2 \neq 0$（ｍｏｄ　ｐ））、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージＭのハッシュ値を計算し、f=Hash(M)とする。

【０１５３】ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関

数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【０１５４】続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【０１５５】

【数１】P=(Ｘａ，Ｙａ),Q=(Ｘｂ，Ｙｂ),R=(Ｘｃ,Ｙｃ)=P+Qとすると、

P≠Qの時（加算）、

Ｘｃ＝λ²－Ｘａ－Ｘｂ

Ｙｃ＝λ×(Ｘａ－Ｘｃ)－Ｙａ

λ＝(Ｙｂ－Ｙａ)／(Ｘｂ－Ｘａ)

P=Qの時（2倍算）、

Ｘｃ＝λ²－２Ｘａ

Ｙｃ＝λ×(Ｘａ－Ｘｃ)－Ｙａ

λ＝(３(Ｘａ)²＋ａ)／(２Ｙａ)

【０１５６】これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、uを2進数展開して1が立っているところに対応する2^i×Ｇ（Ｇをｉ回２倍算した値（ｉはｕのＬＳＢから数えた時のビット位置））を加算する。

【０１５７】ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

【０１５８】ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【０１５９】次に、公開鍵暗号方式を用いた電子署名の検証方法を、図２０を用いて説明する。ステップＳ１１で、Ｍをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$，$4a^3+27b^2\neq 0$（ｍｏｄ　ｐ））、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージＭのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４でh=1/d mod rを計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２＝ｃｈｍｏｄ　ｒを計算する。

【０１６０】ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、ベースポイントＧおよびＫｓ×Ｇを知っているので、図１９のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であることが判明している）。ステップＳ１８でＸｐ　ｍｏｄ　ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【０１６１】電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【０１６２】ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ　ｍｏｄ　ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【０１６３】ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。上述したように、署名付けやハッシュをとるだけでは改竄は可能であるが、検出により実質的に改竄できないことと同様の効果がある。

【０１６４】属性証明書（ＡＣ）要求を受信したサービスプロバイダは、上述の署名検証処理等によって要求データに改竄がないことを確認すると、アプリケーションＩＤで特定されるコンテンツに対応するコンテンツ鍵：Ｋｃを暗号化する。このコンテンツ鍵：Ｋｃの暗号化に適用する鍵は、前述の（ａ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋ、（ｂ）サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋ、（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇのいずれかである。

【０１６５】さらに、サービスプロバイダは、コンテンツの利用条件データ他の必要データを格納し、前述した図５に示す属性証明書を生成する。生成した属性証明書

には、サービスプロバイダの秘密鍵を用いた電子署名が付加される。電子署名の生成処理は、図１９の処理フローと同様の処理に従って実行される。サービスプロバイダによって生成された属性証明書はユーザデバイスに送付され、ユーザデバイスにおいて、上述の図２０の処理フローと同様のシーケンスに従って署名検証処理を実行する。

【０１６６】さらに、必要に応じてユーザデバイスは、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０１６７】属性証明書（ＡＣ）と公開鍵証明書（ＰＫＣ）との関連確認処理、および各証明書の検証処理の詳細について、図を参照して説明する。図２１のフローは、属性証明書（ＡＣ）の検証を実行する際に行なわれる属性証明書（ＡＣ）に関連する公開鍵証明書（ＰＫＣ）の確認処理である。

【０１６８】確認対象の属性証明書（ＡＣ）がセット（Ｓ２１）されると、属性証明書のＡＣ保持者の公開鍵証明書情報（ｈｏｌｄｅｒ）フィールドを抽出（Ｓ２２）し、抽出した公開鍵証明書情報（ｈｏｌｄｅｒ）フィールド内に格納された公開鍵証明書の発行者情報（ＰＫＣ　ｉｓｓｕｅｒ）、公開鍵証明書シリアル番号（ＰＫＣ　ｓｅｒｉａｌ）を確認（Ｓ２３）し、公開鍵証明書の発行者情報（ＰＫＣｉｓｓｕｅｒ）、公開鍵証明書シリアル番号（ＰＫＣ　ｓｅｒｉａｌ）に基づいて公開鍵証明書（ＰＫＣ）を検索（Ｓ２４）して、属性証明書（ＡＣ）に関連付けられた公開鍵証明書（ＰＫＣ）を取得（Ｓ２５）する。

【０１６９】図２１に示すように、属性証明書（ＡＣ）と公開鍵証明書（ＰＫＣ）とは、属性証明書に格納された公開鍵証明書情報（ｈｏｌｄｅｒ）フィールド内の公開鍵証明書発行者情報（ＰＫＣ　ｉｓｓｕｅｒ）、および公開鍵証明書シリアル番号（ＰＫＣ　ｓｅｒｉａｌ）により関連付けがなされている。

【０１７０】次に、図２２を参照して公開鍵証明書（ＰＫＣ）の検証処理について説明する。図２２に示す公開鍵証明書（ＰＫＣ）の検証は、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ルートＣＡ）までの公開鍵証明書の署名検証を行なう連鎖検証処理フローである。まず、検証対象となる公開鍵証明書（ＰＫＣ）をセット（Ｓ３１）し、公開鍵証明書（ＰＫＣ）格納情報に基づいて、公開鍵証明書（ＰＫＣ）署名者を特定（Ｓ３２）する。さらに、検証対象となる証明書連鎖の最上位の公開鍵証明書であるかを判定（Ｓ３３）し、最上位でない場合は、最上位公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ３４）する。最上位公開鍵証明書が取得されセット（Ｓ３５）されると、署名検証に必要な検証鍵（公開鍵）を取得（Ｓ３６）し、検証対象の署名が自己署名であるか否かを判定し（Ｓ３７）、自己署名でない場合は、下位ＰＫＣをセット（Ｓ３９）して、上位の公開鍵証明書から取得した検証鍵（公開鍵）に基づいて署名検証を実行（Ｓ４０）する。なお、ステップＳ３７における自己署名判定において、自己署名の場合は自己の公開鍵を検証鍵とした検証を実行（Ｓ３８）し、ステップＳ４１に進む。

【０１７１】署名検証に成功した場合（Ｓ４１：Ｙｅｓ）は、目的とするＰＫＣの検証が完了したか否かを判定（Ｓ４２）し、完了している場合は、ＰＫＣ検証を終了する。完了していない場合は、ステップＳ３６に戻り、署名検証に必要な検証鍵（公開鍵）の取得、下位の公開鍵証明書の署名検証を繰り返し実行する。なお、署名検証に失敗した場合（Ｓ４１：Ｎｏ）は、ステップＳ４３に進み、エラー処理、例えばその後の手続きを停止する等の処理を実行する。

【０１７２】次に、図２３を参照して属性証明書（ＡＣ）の検証処理（例１）について説明する。まず、検証対象となる属性証明書（ＡＣ）をセット（Ｓ５１）し、属性証明書（ＡＣ）格納情報に基づいて、属性証明書（ＡＣ）の所有者および署名者を特定（Ｓ５２）する。さらに、属性証明書（ＡＣ）の所有者の公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ５３）して、公開鍵証明書の検証処理を実行（Ｓ５４）する。

【０１７３】公開鍵証明書の検証に失敗した場合（Ｓ５５でＮｏ）は、ステップＳ５６に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ５５でＹｅｓ）は、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ５７）して、公開鍵証明書の検証処理を実行（Ｓ５８）する。公開鍵証明書の検証に失敗した場合（Ｓ５９でＮｏ）は、ステップＳ６０に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ５９でＹｅｓ）は、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書から公開鍵を取り出し（Ｓ６１）て、取り出した公開鍵を用いて属性証明書（ＡＣ）の署名検証処理を実行（Ｓ６２）する。署名検証に失敗した場合（Ｓ６３でＮｏ）は、ステップＳ６４に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合（Ｓ６３でＹｅｓ）は、属性証明書検証を終了し、その後の処理、例えば属性証明書内の暗号化コンテ

ンツ鍵の取得等に移行する。

【０１７４】次に、図２４を参照して属性証明書（ＡＣ）の検証処理（例２）について説明する。本例は、自デバイス内に属性証明書（ＡＣ）の検証処理に必要となる公開鍵証明書が格納されているか否かを判定し、公開鍵証明書が格納されている場合は、その検証を省略することとした例である。まず、検証対象となる属性証明書（ＡＣ）をセット（Ｓ７１）し、属性証明書（ＡＣ）格納情報に基づいて、属性証明書（ＡＣ）の所有者および署名者を特定（Ｓ７２）する。さらに、属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに格納保存されていないかを検索（Ｓ７３）する。保存されている場合（Ｓ７４でＹｅｓ）は、属性証明書（ＡＣ）の所有者の公開鍵証明書を取り出し（Ｓ７５）て、ステップＳ８１に進む。

【０１７５】属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに保存されていない場合（Ｓ７４でＮｏ）は、属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）を直接あるいはリポジトリなどから取得（Ｓ７６）して、属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）の検証処理を実行（Ｓ７７）する。公開鍵証明書の検証に失敗した場合（Ｓ７８でＮｏ）は、ステップＳ７９に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ７８でＹｅｓ）は、公開鍵証明書の検証結果を保存（Ｓ８０）した後、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに格納保存されていないかを検索（Ｓ８１）する。保存されている場合（Ｓ８２でＹｅｓ）は、属性証明書（ＡＣ）の署名者の公開鍵証明書を取り出し（Ｓ８３）て、ステップＳ８８に進む。

【０１７６】属性証明書（ＡＣ）の署名者の公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに保存されていない場合（Ｓ８２でＮｏ）は、属性証明書（ＡＣ）の署名者の公開鍵証明書（ＰＫＣ）を直接あるいはリポジトリなどから取得（Ｓ８４）して、属性証明書（ＡＣ）の署名者の公開鍵証明書（ＰＫＣ）の検証処理を実行（Ｓ８５）する。公開鍵証明書の検証に失敗した場合（Ｓ８６でＮｏ）は、ステップＳ８７に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ８６でＹｅｓ）は、公開鍵証明書から属性証明書（ＡＣ）の署名検証に適用する鍵（公開鍵）を取り出し（Ｓ８８）、属性証明書（ＡＣ）の署名検証処理を実行（Ｓ８９）する。署名検証に失敗した場合（Ｓ９０でＮｏ）は、ステップＳ９１に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合（Ｓ９０でＹｅｓ）は、属性証明書検証を終了し、その後の処理、例えば属性証明書内の暗号化コンテンツ鍵の取得等に移行する。

【０１７７】ユーザデバイスによる属性証明書の検証がなされると、属性証明書はユーザデバイス内のセキュリティチップのメモリ、あるいはセキュリティチップ外のユーザデバイス制御部の管理下の外部メモリに格納され、コンテンツの利用時に、属性証明書内の暗号化コンテンツ鍵の取得、復号化処理を実行することになる。属性証明書から暗号化されたコンテンツ鍵を取得して復号する処理について、以下説明する。

【０１７８】（ａ）ＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを適用した場合

まず、前述の（ａ）ＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋをコンテンツ鍵：Ｋｃの暗号化に適用し、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納した属性証明書に基づくコンテンツ利用処理について説明する。

【０１７９】ＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋは、サービスプロバイダ管理領域に格納され、ユーザは前述した認証情報（パスワード）入力により、この鍵を取り出して利用することができる。従って、コンテンツ鍵：Ｋｃはサービスプロバイダに接続することなくオフライン処理として取得可能であり、コンテンツの復号が可能となる。

【０１８０】図２５に属性証明書からの暗号化コンテンツ鍵取得、復号、コンテンツ鍵によるコンテンツ復号化処理のシーケンスを説明する図を示す。

【０１８１】図２５のシーケンス図に従って説明する。図２５は左からセキュリティチップ内部のメモリ、セキュリティチップ制御部、ユーザデバイス制御部の処理を示している。まず、ユーザデバイスに対してユーザの入力したコンテンツ識別情報としてのアプリケーションＩＤをセキュリティチップ制御部に送信し、メモリからアプリケーションＩＤに対応する属性証明書（ＡＣ）を取得する。ユーザデバイスでは、アプリケーションＩＤに対応する属性証明書であるかの検証を行ない、セキュリティチップ制御部に属性証明書をセットし、コンテンツ鍵：Ｋｃの取得（復号）処理を要求する。

【０１８２】セキュリティチップ制御部は、属性証明書の署名検証を実行し、データ改竄のないことを確認し、属性証明書内に格納された暗号化コンテンツ鍵：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを適用して復号化処理を実行し、コンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０１８３】次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツを、セキュリティチップ制御部を介してメモリから取得す

る。暗号化コンテンツがセキュリティチップ内のメモリではなく、外部メモリ（例えばハードディスク）等に格納されている場合は、外部メモリから暗号化コンテンツを取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力する。

【０１８４】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、暗号化コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋを用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【０１８５】（ｂ）サービスプロバイダの保有する秘密鍵（共通鍵系）：ＳＰ．Ｓｔｏ．Ｋを適用した場合

次に、前述の（ｂ）サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋをコンテンツ鍵：Ｋｃの暗号化に適用し、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］を格納した属性証明書に基づくコンテンツ利用処理について説明する。

【０１８６】サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋは、サービスプロバイダが保有し、ユーザデバイスには格納されていない鍵である。従って、ユーザデバイスがコンテンツ鍵：Ｋｃを取得するためには、サービスプロバイダに接続して、コンテンツ鍵の復号化処理をサービスプロバイダに対して要求することが必要となり、オンライン処理によるコンテンツ復号を実行することとなる。

【０１８７】図２６に属性証明書からのコンテンツ鍵取得、復号、コンテンツ鍵によるコンテンツ復号化処理のシーケンスを説明する図を示す。

【０１８８】図２６のシーケンス図に従って説明する。図２６は左からセキュリティチップ内部のメモリ、セキュリティチップ制御部、ユーザデバイス制御部、サービスプロバイダにおける処理を示している。

【０１８９】まず、ユーザデバイスに対してユーザの入力したコンテンツ識別情報としてのアプリケーションＩＤをセキュリティチップ制御部に送信し、メモリからアプリケーションＩＤに対応する属性証明書（ＡＣ）を取得する。ユーザデバイスでは、アプリケーションＩＤに対応する属性証明書であるかの検証を行ない、セキュリティチップ制御部に属性証明書をセットし、コンテンツ鍵：Ｋｃの取得（復号）処理を要求する。

【０１９０】セキュリティチップ制御部は、属性証明書の検証の後、属性証明書の発行元であるサービスプロバイダに対してユーザデバイスを介して接続し、セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。

【０１９１】相互認証が成立すると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０１９２】セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、サービスプロバイダは、自己の所有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを用いて、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号化処理を実行し、コンテンツ鍵：Ｋｃを取り出す。さらに、取り出したコンテンツ鍵：Ｋｃを先の相互認証処理において生成したセッションキー（Ｋｓｅｓ）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【０１９３】セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、［Ｋｓｅｓ（Ｋｃ）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。

【０１９４】コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツをセキュリティチップ制御部を介してメモリから取得する。暗号化コンテンツがセキュリティチップ内のメモリではなく、外部メモリ（例えばハードディスク）等に格納されている場合は、外部メモリから暗号化コンテンツを取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力する。

【０１９５】（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇを適用した場合
次に、システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇを、コンテンツ鍵：Ｋｃの暗号化に間接的に適用して属性証明書に格納する処理形態について説明する。このグローバル共通鍵を利用する形態は、ユーザデバイスにおいてのみコンテンツ鍵：Ｋｃを取り出すことを可能とし、コンテンツの配信を実行するサービスプロバイダはコンテンツ鍵の取り出しを不可能とすることで、システムホルダの許可なくコンテンツが配布、利用されることを防止し、システムホルダ（ＳＨ）による管理されたコンテンツ配信を行なうことが可能となる。

【０１９６】具体的には、サービスプロバイダに対してコンテンツを提供するコンテンツクリエータの有するコンテンツ製作者鍵、コンテンツ配信を行なうサービスプロバイダの有するコンテンツ配信者鍵、そしてシステムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇの各鍵を組み合わせた暗号化処理を行なった暗号化鍵データを属性証明書に格納する。

【０１９７】図２７に、グローバル共通鍵：Ｋｇをコンテンツ鍵：Ｋｃの暗号化に間接的に適用してコンテンツ鍵：Ｋｃの暗号化データを属性証明書に格納して配布する処理の詳細を説明する図を示す。

【０１９８】図２７には、コンテンツ配信のプラットホームを構築、管理するシステムホルダ３０１、コンテンツ配信を実行するサービスプロバイダ（ＣＤ：コンテンツディストリビュータ）３０２、コンテンツを生成または管理し、サービスプロバイダ３０２に対して暗号化コンテンツを提供するコンテンツクリエータ３０３、サービスプロバイダ３０２からコンテンツを受領するエンドエンティティとしてのユーザデバイス３０４を示している。なお、ユーザデバイス３０４は、前述の（ａ），（ｂ）の例と同様、セキュリティチップを有し、セキュリティチップ内のメモリ領域にはサービスプロバイダ管理領域が生成されている。

【０１９９】図２７の処理について説明する。まず、コンテンツクリエータ３０３は、配信対象となるコンテンツを暗号化するための鍵：Ｋｃを例えば乱数により生成し、生成したコンテンツ鍵（共通鍵系）：Ｋｃを用いて、（１）コンテンツを暗号化してサービスプロバイダ３０２に提供する。

【０２００】さらに、システムホルダ３０１は、（２）コンテンツクリエータ３０３から、コンテンツクリエータ３０３の保有するコンテンツクリエータ鍵（共通鍵系）：Ｋｃｃを受信し、（３）サービスプロバイダ（ＣＤ：コンテンツディストリビュータ）３０２からサービスプロバイダ３０２の保有するサービスプロバイダ鍵（共通鍵系）：Ｋｃｄを受信する。なお、これらの鍵は事前に受け渡しを行なってもよい。

【０２０１】システムホルダ３０１は、コンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化する。すなわち暗号化鍵データ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］を生成し、（４）これをコンテンツクリエータ３０３に送付する。なお、［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］は事前に受け渡しを行なってもよい。グローバル共通鍵：Ｋｇは、システムホルダ３０１と、ユーザデバイス３０４が共有する鍵である。ユーザデバイス３０４には、（５）デバイス製造時、デバイス販売時まで、あるいは少なくともコンテンツの購入開始前までに、１以上のグローバル共通鍵：Ｋｇ１～Ｋｇｎが格納され、これらはシステムホルダの管理の下に更新処理が実行される。更新処理については、後述する。

【０２０２】コンテンツクリエータ３０３は、コンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］を生成し、（６）これをサービスプロバイダ３０２に対して送信するとともに、システムホルダ３０１から受信した、コンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化した暗号化鍵データ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］をサービスプロバイダ３０２に対して送信する。なお、［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］は事前に受け渡しを行なってもよい。

【０２０３】ユーザデバイス３０４がサービスプロバイダ３０２に対して（７）コンテンツ購入要求を行なうと、（８）サービスプロバイダは、要求コンテンツに対応する属性証明書を生成して、ユーザデバイス３０４に送信する。生成する属性証明書（ＡＣ）には、前述の暗号鍵データ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］、すなわち、コンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化したデータ、および、コンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］が格納される。その他、コンテンツの利用条件等のデータが格納され、サービスプロバイダ３０２の電子署名がなされてユーザデバイス３０４に送信される。ユーザデバイス３０４は、受信した属性証明書（ＡＣ）をメモリに格納する。

【０２０４】コンテンツの利用時には、ユーザデバイス３０４は、サービスプロバイダ３０２との間で（９）相互認証を行なった後、（１０）先に受信済みの属性証明書（ＡＣ）をサービスプロバイダ３０２に送信する。相互認証処理は、ユーザデバイスのセキュリティチップとサービスプロバイダ間の相互認証処理として実行され

る。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。

【０２０５】属性証明書には、前述のコンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化したデータ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］、および、コンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］が格納されている。

【０２０６】セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（１１）サービスプロバイダは、自己の所有するサービスプロバイダ鍵：Ｋｃｄを、相互認証時に生成したセッション鍵：Ｋｓｅｓで暗号化して、暗号化鍵データ［Ｋｓｅｓ（Ｋｃｄ）］を生成し、これをユーザデバイスに送信する。

【０２０７】ユーザデバイス３０４のセキュリティチップ制御部は、（１２）サービスプロバイダ３０２から受信した暗号化鍵データ［Ｋｓｅｓ（Ｋｃｄ）］について、セッションキーを用いた復号化処理を実行してサービスプロバイダ鍵：Ｋｃｄを取得する。なお、サービスプロバイダ鍵：Ｋｃｄを事前にサービスプロバイダメモリ領域に保管しておいてもよい。

【０２０８】ユーザデバイス３０４のセキュリティチップ制御部は、次に、（１３）属性証明書中のコンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化したデータ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］について、まず、自己の所有するグローバル共通鍵：Ｋｇで復号し、［Ｋｃｄ（Ｋｃｃ）］を取得する。さらに、（１４）サービスプロバイダ３０２から受信した暗号化鍵データの復号により取得したサービスプロバイダ鍵：Ｋｃｄを適用した復号化処理により、コンテンツクリエータ鍵：Ｋｃｃを取得する。

【０２０９】さらに、（１５）ユーザデバイス３０４のセキュリティチップ制御部は、属性証明書中のコンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］を取り出して、前記処理によって取得したコンテンツクリエータ鍵：Ｋｃｃを適用した復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。

【０２１０】コンテンツ鍵：Ｋｃの取得に成功すると、ユーザデバイス３０４のセキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０２１１】ユーザデバイス３０４は、サービスプロバイダ３０２から取得した暗号化コンテンツ（（１６）の処理）をセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行する。

【０２１２】なお、上述の各エンティティ間における鍵、暗号化鍵等のデータ送受信の前には、データ送受信を実行するエンティティ間で相互認証を実行し、認証成立を条件としたデータ送受信を行なうことが好ましく、また送受信データはセッションキーで暗号化し、署名を付与した構成とすることが好ましい。

【０２１３】このように、グローバル共通鍵は、ユーザデバイスとシステムホルダのみが所有し、その他のエンティティは保有することがなく、他のエンティティでは取得不可能な鍵として構成される。従って、サービスプロバイダにおいてもコンテンツ鍵の取得は不可能であり、システムホルダの許可のないコンテンツ鍵の流通、コンテンツの流通が防止可能となる。

【０２１４】グローバル共通鍵は、必要に応じて更新される。更新を実行するのは、システムホルダの管理下にあるサポートセンタである。サポートセンタとユーザデバイス間で実行されるグローバル共通鍵更新処理シーケンスを図２８に示す。ユーザデバイスのセキュリティチップ内のメモリ領域には、２つのグローバル共通鍵Ｋｇ１，Ｋｇ２が格納されているものとする。これらのいずれかを使用して属性証明書内の鍵データの暗号化がなされ、復号化処理が実行される。あるいは例えばトリプルＤＥＳアルゴリズムを適用して２つの鍵を用いて属性証明書内の鍵データの暗号化を行ない、２つの鍵を用いた復号化処理を実行する構成としてもよい。

【０２１５】図２８の処理シーケンスに示す各処理について説明する。図２８は左からセキュリティチップ制御部、ユーザデバイス制御部、システムホルダの管理下にあるサポートセンタにおける処理を示している。

【０２１６】まず、ユーザデバイス制御部がグローバル共通鍵：Ｋｇ更新要求をセキュリティチップ制御部に送信すると、セキュリティチップ制御部は、システムホルダの管理下にあるサポートセンタに対してユーザデバイスを介して接続し、セキュリティチップとサポートセンタ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認

証処理において、セキュリティチップと、サポートセンタはセッション鍵（Ｋｓｅｓ）を共有する。

【０２１７】相互認証が成立すると、セキュリティチップの制御部は、サポートセンタに対してグローバル共通鍵：Ｋｇ更新要求を出力する。サポートセンタは、すでに生成済みの更新用グローバル共通鍵：Ｋｇ３、あるいは要求に応じて生成したグローバル共通鍵：Ｋｇ３を認証処理において生成したセッション鍵：Ｋｓｅｓで暗号化し、暗号化鍵データ：［Ｋｓｅｓ（Ｋｇ３）］をユーザデバイスのセキュリティチップに対して送信する。

【０２１８】セキュリティチップの制御部は、サポートセンタからセッションキーで暗号化されたグローバル共通鍵：Ｋｇ３、すなわち、［Ｋｓｅｓ（Ｋｇ３）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してグローバル共通鍵：Ｋｇ３を取得する。

【０２１９】グローバル共通鍵：Ｋｇ３の取得に成功すると、セキュリティチップ制御部は、グローバル共通鍵：Ｋｇ１を、取得したグローバル共通鍵：Ｋｇ３に置き換える。これにより、ユーザデバイスの保有するグローバル共通鍵は、Ｋｇ２、Ｋｇ３となる。ユーザデバイスの保有するグローバル共通鍵は、その順序関係も含めて意味があるため、［Ｋｇ１，Ｋｇ２］の順序関係も併せて［Ｋｇ２，Ｋｇ３］と修正する。グローバル共通鍵は、鍵データと共にユーザデバイス内で保持されている順序関係も合わせてデータを保持しているものとする。

【０２２０】図２９は、ユーザデバイスとサポートセンタが直接データ送受信を行なうことなく、サービスプロバイダが仲介を行なってグローバル共通鍵の更新を実行する処理シーケンス例を示した図である。

【０２２１】図２９の処理シーケンスに示す各処理について説明する。図２９は左からセキュリティチップ制御部、ユーザデバイス制御部、サービスプロバイダ、システムホルダの管理下にあるサポートセンタにおける処理を示している。

【０２２２】サポートセンタでは、更新される新たなグローバル共通鍵：Ｋｇ３を事前生成し、グローバル共通鍵：Ｋｇ３をすでにユーザデバイスに配布済みのグローバル共通鍵：Ｋｇ２で暗号化してデータ：［Ｋｇ２（Ｋｇ３）］を生成し、これに、サポートセンタの秘密鍵：Ｋｓｓで署名を付してサービスプロバイダに送付する。サービスプロバイダは、データ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［Ｋｓｓ］を有する。なお、Ａ，Ｓｉｇ［Ｂ］は、データＡに鍵Ｂで署名を付加したデータ構成を示すものとする。

【０２２３】次に、ユーザデバイス制御部がグローバル共通鍵：Ｋｇ更新要求をセキュリティチップ制御部に送信すると、セキュリティチップ制御部は、サービスプロバイダに対してユーザデバイスを介して接続し、セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。

【０２２４】相互認証が成立すると、セキュリティチップの制御部は、サービスプロバイダに対してグローバル共通鍵：Ｋｇ更新要求を出力する。サービスプロバイダはサポートセンタから受信済みのデータ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［ＳｕＣ］をユーザデバイスのセキュリティチップに対して送信する。

【０２２５】セキュリティチップの制御部は、サービスプロバイダから、サポートセンタからのデータ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［ＳｕＣ］の転送を受けると、署名検証処理を実行し、データ改竄のないことを確認した後、自己の所有するグローバル共通鍵：Ｋｇ２で暗号化されたグローバル共通鍵：Ｋｇ３、すなわち、［Ｋｇ２（Ｋｇ３）］に対して、グローバル共通鍵：Ｋｇ２を用いた復号化処理を実行してグローバル共通鍵：Ｋｇ３を取得する。なお、サポートセンタの署名検証にサポートセンタの公開鍵を適用する場合は、サポートセンタの公開鍵証明書をユーザデバイスに対してデータ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［ＳｕＣ］とともに送信するか、あるいはユーザデバイスに予め配布しておく。

【０２２６】グローバル共通鍵：Ｋｇ３の取得に成功すると、セキュリティチップ制御部は、メモリの鍵格納領域、例えば前述のデバイス管理領域内のグローバル共通鍵：Ｋｇ１書き込み領域にグローバル共通鍵：Ｋｇ３を上書きする。この更新処理により、ユーザデバイスの保有するグローバル共通鍵は、Ｋｇ２、Ｋｇ３の２つに更新される。

【０２２７】［デコーダを利用した復号化処理］暗号化コンテンツ、あるいは暗号化コンテンツ鍵は、専用の復号化処理機能を持つデコーダに処理を実行させる構成とすると処理の高速化が可能となる。ただし、デコーダはセキュリティチップと独立したハード構成を持つため、デコーダの信頼性を確認した上でデコーダ内でのコンテンツ鍵、コンテンツの復号化を行なうことが必要となる。以下、デコーダを用いた暗号化コンテンツ、あるいは暗号化コンテンツ鍵の復号化処理について図を参照して説明する。

【０２２８】図３０にユーザデバイスにセキュリティチップと、デコーダを有する場合のコンテンツ鍵、コンテンツの復号化処理シーケンスを説明する図を示す。

【０２２９】ユーザデバイスは、セキュリティチップ２１０と、デコーダ２８０、ハードディスク、フラッシュメモリ等からなるメモリ部２２２と、上位ソフトウェア

によりセキュリティチップ２１０と、デコーダ２８０、メモリ部２２２に対してデータ入出力、各種処理実行命令を行なうユーザデバイス側制御部２２１がある。

【０２３０】コンテンツ復号化処理時のシーケンスについて説明する。まず、ユーザによる入力手段の操作により、コンテンツを指定したコンテンツ利用要求がユーザデバイス側制御部２２１に入力されると、ユーザデバイス側制御部２２１は、メモリ部２２２に格納された指定コンテンツに対応する属性証明書（ＡＣ）を検索する。検索により抽出された属性証明書（ＡＣ）はセキュリティチップ２１０に転送され、セキュリティチップ２１０内で、属性証明書（ＡＣ）の検証処理が実行される。

【０２３１】属性証明書（ＡＣ）検証処理に成功すると、セキュリティチップ２１０とデコーダ２８０間において相互認証およびセッション鍵の共有処理が実行される。相互認証が成立した後、セキュリティチップ２１０は、属性証明書（ＡＣ）から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダ２８０と共有したセッション鍵を用いてコンテンツ鍵を再暗号化してデコーダ２８０に送信する。暗号化コンテンツ鍵を受信したデコーダ２８０は、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得する。

【０２３２】次に、ユーザデバイス側制御部２２１は、メモリ部２２２に格納された暗号化コンテンツを検索して取り出し、デコーダ２８０に送信する。デコーダ２８０は、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行する。

【０２３３】上述したデコーダを適用した処理では、コンテンツ鍵はセキュリティチップ２１０内では使用されない。また、デコーダは、暗号化コンテンツを復号化して、アナログ出力として音声または映像データを外部出力する。なお、属性証明書（ＡＣ）には、認証するデコーダのＩＤや認証方式を記述してもよく、この場合、セキュリティチップ２１０は、相互認証時にデコーダが属性証明書（ＡＣ）に記述されたデコーダＩＤや認証方式に適合するか否かを判定して、適合する場合にのみコンテンツ鍵をデコーダに出力する。

【０２３４】デコーダを用いた処理シーケンスについて図３１を用いて説明する。図３１において、左からセキュリティチップ、上位ソフトウェア（ユーザデバイス側制御部）、デコーダの各処理を示している。

【０２３５】利用者による入力手段の操作により、コンテンツを指定したコンテンツ利用要求が上位ソフトウェア（ユーザデバイス側制御部）に入力されると、上位ソフトウェア（ユーザデバイス側制御部）は指定コンテンツに対応するアプリケーションＩＤを取得し、アプリケーションＩＤに基づいて、ハードディスク等のメモリに格納されたアプリケーションＩＤに対応する属性証明書（ＡＣ）を検索する。

【０２３６】検索により抽出された属性証明書（ＡＣ）は、属性証明書（ＡＣ）検証処理命令とともにセキュリティチップに転送され、セキュリティチップは、属性証明書（ＡＣ）の検証処理を実行し、属性証明書（ＡＣ）検証処理に成功すると、セキュリティチップは、属性証明書（ＡＣ）から暗号化コンテンツ鍵を取り出して、復号化処理を実行するとともに、上位ソフトウェア（ユーザデバイス側制御部）に応答メッセージを出力する。

【０２３７】次に、セキュリティチップとデコーダ間において、上位ソフトウェア（ユーザデバイス側制御部）を介して相互認証およびセッション鍵の共有処理が実行される。相互認証が成立した後、セキュリティチップは、属性証明書（ＡＣ）から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダと共有したセッション鍵を用いてコンテンツ鍵を再暗号化してデコーダに送信する。暗号化コンテンツ鍵を受信したデコーダは、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得する。

【０２３８】次に、ユーザデバイス側制御部は、メモリに格納された暗号化コンテンツを検索して取り出し、デコーダに送信する。デコーダは、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行する。

【０２３９】次に、デコーダを用いたコンテンツ復号化処理について、図３２のフローを参照して説明する。

【０２４０】ステップＳ１０１において、利用者による入力手段の操作により、コンテンツを指定したコンテンツ利用要求が上位ソフトウェア（ユーザデバイス側制御部）に入力されると、ステップＳ１０２において、上位ソフトウェア（ユーザデバイス側制御部）は指定コンテンツに対応するアプリケーションＩＤを取得し、ステップＳ１０３において、アプリケーションＩＤに基づいて、ハードディスク等のメモリに格納されたアプリケーションＩＤに対応する属性証明書（ＡＣ）を検索する。検索により抽出された属性証明書（ＡＣ）は、ステップＳ１０４において、属性証明書（ＡＣ）検証処理命令とともにセキュリティチップに転送され、セキュリティチップは、ステップＳ１０５において、属性証明書（ＡＣ）の検証処理を実行し、属性証明書（ＡＣ）検証処理に成功すると、セキュリティチップは、属性証明書（ＡＣ）から暗号化コンテンツ鍵を取り出して、復号化処理を実行する。また、ステップＳ１０６において、上位ソフトウェア（ユーザデバイス側制御部）に応答メッセージを出力する。

【０２４１】属性証明書（ＡＣ）検証処理に成功しなかった場合は、その後の処理は中止される。検証成功の場合は、セキュリティチップとデコーダ間において、上位ソフトウェア（ユーザデバイス側制御部）を介して相互認証およびセッション鍵の共有処理が実行される。具体的には、ステップＳ１０８において、上位ソフトウェア

（ユーザデバイス側制御部）からセキュリティチップに第１認証コマンドが発行され、ステップＳ１０９においてセキュリティチップからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信し、さらに、ステップＳ１１０において、上位ソフトウェア（ユーザデバイス側制御部）からデコーダに第２認証コマンドが発行され、ステップＳ１１１においてデコーダからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信し、さらに、ステップＳ１１２において、上位ソフトウェア（ユーザデバイス側制御部）からセキュリティチップに第３認証コマンドが発行され、ステップＳ１１３においてセキュリティチップからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信する処理によって、セキュリティチップによるデコーダの認証処理が実行される。認証処理が失敗した場合（Ｓ１１４でＮＧ）は、その後の処理は中止され、成功した場合は、ステップＳ１１５に進む。

【０２４２】ステップＳ１１５において、上位ソフトウェア（ユーザデバイス側制御部）からデコーダに第４認証コマンドが発行され、ステップＳ１１６においてデコーダからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信する。この処理によって、デコーダによるセキュリティチップの認証の成否が判定される。認証処理が失敗の場合（Ｓ１１７でＮＧ）は、その後の処理は中止され、成功した場合は、ステップＳ１１８に進む。

【０２４３】ステップＳ１１８において、セキュリティチップは、属性証明書（ＡＣ）から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダと共有したセッション鍵を用いてコンテンツ鍵を再暗号化（Ｓ１１８）して、上位ソフトウェア（ユーザデバイス側制御部）に送信（Ｓ１１９）する。上位ソフトウェア（ユーザデバイス側制御部）は、受信した暗号化コンテンツ鍵をデコーダに送信（Ｓ１２０）する。

【０２４４】暗号化コンテンツ鍵を受信したデコーダは、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得（Ｓ１２１）する。上位ソフトウェア（ユーザデバイス側制御部）は、メモリに格納された暗号化コンテンツを検索（Ｓ１２２）して取り出し、デコーダに送信（Ｓ１２３）する。デコーダは、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行（Ｓ１２４）する。

【０２４５】このように、デコーダを用いた復号化処理においては、セキュリティチップとデコーダ間の相互認証が実行されて、相互認証の成立を条件として、セッション鍵で暗号化したコンテンツ鍵がデコーダに出力する構成としたので、信頼される機器においてのみ復号が実行され、正当なコンテンツ利用を確保することができる。

【０２４６】［コンテンツの利用制限］先に説明したように、コンテンツの利用制限情報を格納したコンテンツ対応の属性証明書中の属性情報フィールドに格納されるコンテンツ利用条件関連情報には、サービスプロバイダの提供するコンテンツの利用制限回数、利用期限等の様々な利用条件が含まれる。すなわち、以下の情報である。

条件：オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかを示す情報

有効期限：期間制限の場合の有効期限情報

利用制限回数：回数制限の場合の利用可能回数

【０２４７】コンテンツを買い切りし、買い切り以後のコンテンツ利用をフリーとするコンテンツに対応する属性証明書は、上記条件が買い切りとして設定される。利用期間を設定したコンテンツに対応する属性証明書は、上記条件が期間制限として設定され、有効期限が設定される。利用回数制限を設定したコンテンツに対応する属性証明書は、上記条件が回数制限として設定され、利用制限回数に設定値（回数値）が設定される。なお、回数制限処理の場合には、ユーザデバイス内で利用可能回数を管理してコンテンツ利用を実行するオフライン回数制限と、サービスプロバイダにおいて回数検証をした後、属性証明書に記録された設定回数以内のコンテンツ利用を許可するオンライン回数制限がある。また期間制限と回数制限の両制限を伴うコンビネーション制限態様もある。ユーザデバイスでは、属性証明書に記録されたこれらの態様に従ってコンテンツが利用される。これらの具体的な処理態様について、以下、説明する。

【０２４８】ユーザデバイスにおいてコンテンツを利用するためには、利用対象となるコンテンツに対応する属性証明書中から暗号化コンテンツ鍵を取り出して復号化処理を実行してコンテンツ鍵：Ｋｃを取得することが必要となる。このコンテンツ鍵の取得処理には、デバイスのセキュリティチップ内で実行するオフライン処理、サービスプロバイダに属性証明書を送付して復号を依頼するオンライン処理があることは先に述べた通りである。属性証明書に記載されたコンテンツの利用条件に従ったコンテンツ利用処理においても、利用条件をユーザデバイス内で確認するオフライン処理、サービスプロバイダでの確認を必要とするオンライン処理がある。これらのどちらを適用するかは、属性証明書の属性情報フィールドの記載に従って決定する。

【０２４９】図３３にコンテンツ利用時におけるユーザデバイスで実行される属性証明書（ＡＣ）の利用処理フローを示す。処理フローの各ステップについて説明する。

【０２５０】ユーザデバイスは、利用対象コンテンツに対応する属性証明書をアプリケーションＩＤ（コンテンツ識別情報）に基づいて選択すると、まず、属性証明書

のフォーマット確認処理を実行（Ｓ２０１）する。属性証明書に必要事項が記録され、証明書の有効期限が有効であるか等である。フォーマット確認処理が済むと、ステップＳ２０２において署名検証が実行される。先にも説明したように属性証明書には、属性証明書発行者（例えばサービスプロバイダ）の電子署名が付加されており、ユーザデバイスは、属性証明書発行者の公開鍵証明書から公開鍵を取り出して署名検証処理（図２０参照）を行なう。なお、この際使用する公開鍵証明書の検証、連鎖的公開鍵証明書の検証処理も必要に応じて実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０２５１】ステップＳ２０２の署名検証処理過程において、検証が成立し、属性証明書に改竄がないと判定された場合はステップＳ２０３に進む。一方、ステップＳ２０２の署名検証処理過程において、検証が非成立となり、属性証明書に改竄ありと判定された場合は、ステップＳ２０５に進み、その属性証明書を適用した処理は実行されず、以降の処理、すなわちコンテンツ利用処理が中止される。

【０２５２】属性証明書に改竄がないと判定され、ステップＳ２０３に進むと、属性証明書内の属性情報フィールド内のコンテンツ利用条件情報を取得する。すなわち、オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかである。この条件に従って、ステップＳ２０４のオンライン処理であるか、オフラインである場合は、ステップＳ２０６において買い切りか、回数制限であるかが判定される。

【０２５３】ステップＳ２０４において、オンライン利用であると判定されると、先に図２６を用いて説明したと同様、属性証明書をサービスプロバイダに送付して属性証明書内の利用制限情報の検証が実行される。オンライン処理の場合は、期間制限、または回数制限のいずれかであり、サービスプロバイダはこれらのコンテンツ利用条件情報を属性証明書から取得して利用制限内のコンテンツ利用請求であれば、コンテンツ鍵の取得を可能とする処理を行なう。利用制限を超えたコンテンツ利用請求であれば、コンテンツ鍵の取得を可能とする処理を実行せず、コンテンツ利用不可であるメッセージをユーザデバイスに送信する。

【０２５４】また、ステップＳ２０４において、オフライン利用であると判定され、ステップＳ２０６で買い切りコンテンツであると判定された場合には、属性証明書には、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋで暗号化されたコンテンツ鍵データ：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］が格納されており、ユーザデバイスでは、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得して、コンテンツの復号によりコンテンツを利用する。

【０２５５】さらに、ステップＳ２０４において、オフライン利用であると判定され、ステップＳ２０６で回数制限のコンテンツであると判定された場合には、ユーザデバイス内で、属性証明書の設定条件に基づいて回数管理を実行して、コンテンツ利用の可否判定を実行した後、利用可であるとの判定結果の取得を条件として、属性証明書内に格納された暗号化コンテンツ鍵の復号化処理を実行し、かつ、デバイス内で管理するコンテンツ利用回数管理データの更新処理等を実行する。このためにデバイス内にコンテンツ利用回数の管理データを持つことが必要となる。

【０２５６】ステップＳ２０７の利用回数管理データのインポート処理は、コンテンツ利用回数の管理データ生成処理である。なお、利用回数管理データのインポート処理は、属性証明書に基づいて実行される。コンテンツ利用回数の管理態様には、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する２つの態様がある。これらの詳細については後述する。ステップＳ２０８の属性証明書適用完了メッセージ生成ステップは、上述のＳ２０７の利用回数管理データのインポート処理が完了したことをセキュリティチップからセキュリティチップ外のユーザデバイスに通知する処理である。

【０２５７】以下、属性証明書（ＡＣ）に記載されたコンテンツ利用条件を以下の４態様に区別して、順次、説明する。

（Ａ）オンライン－利用期間制限コンテンツ
（Ｂ）オンライン－利用回数制限コンテンツ
（Ｃ）オフライン－買い切りコンテンツ
（Ｄ）オフライン－利用回数制限コンテンツ

【０２５８】（Ａ）オンライン－利用期間制限コンテンツ

まず、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用期間が制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図３４のシーケンス図に従って説明する。

【０２５９】図３４に示す処理シーケンスは、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制

御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０２６０】図３４では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ｃ）の相互認証処理、（ｄ）のコンテンツ取得処理は共通に実行される。

【０２６１】まず、（ａ）の処理から説明する。（ａ１）ユーザデバイス制御部は、利用対象コンテンツに対応する属性証明書の検索をセキュリティチップ制御部に要求する。（ａ２）セキュリティチップ制御部は、チップのメモリに格納済みの属性証明書のリストをユーザデバイス制御部に出力し、（ａ３）ユーザデバイスでは付属のブラウザによりリストを表示する。（ａ４）ユーザは表示されたリストから利用予定コンテンツに対応する属性証明書（ＡＣ）を指定し、読み出し命令をセキュリティチップ制御部に送信する。（ａ５）セキュリティチップ制御部は、指定された属性証明書を内部メモリから読み出してユーザデバイス制御部に出力し、（ａ６）ユーザデバイスでは付属のブラウザにより属性証明書を表示し、属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０２６２】属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合は、（ｂ）の処理となる。（ｂ１）ユーザデバイス制御部は、利用対象コンテンツに対応する属性証明書の検索を実行し、（ｂ２）ユーザデバイスでは付属のブラウザにより表示されたＡＣリストから利用予定コンテンツに対応する属性証明書（ＡＣ）を指定し、（ｂ３）読み出して属性証明書を表示し、（ｂ４）属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０２６３】上記（ａ）、（ｂ）のいずれかの処理によって取得されたサービスプロバイダ識別子（ＳＰ　ＩＤ）は、サービスプロバイダ管理領域から、相互認証に必要な情報を取得するために用いられる。前述したように、サービスプロバイダ管理領域へのアクセスにはサービスプロバイダ毎に設定されたパスワード入力が必要であり、ユーザは、属性証明書から取得したサービスプロバイダ識別子（ＳＰ　ＩＤ）に対応するパスワード入力により、サービスプロバイダ管理領域へのアクセスを実行し、図３４の（ｃ１）に示すセキュリティチップとサービスプロバイダ間の相互認証処理を実行する。

【０２６４】この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サポートセンタはセッション鍵（Ｋｓｅｓ）を共有する。相互認証が成立すると、次に、図３４（ｄ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０２６５】（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オンライン期間制限である。

【０２６６】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。

【０２６７】さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０２６８】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、利用条件としてオンライン期間制限コンテンツであることが記録され、また有効期限データが格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０２６９】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、属性証明書に格納された利

用条件データ、有効期限データを確認する。属性証明書に記録されている利用条件としての有効期限内のコンテンツ利用要求であると判定されると、属性証明書中に格納されたコンテンツの復号に適用するコンテンツ鍵：Ｋｃの暗号化データ：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号を実行する。

【０２７０】サービスプロバイダは、自己の所有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを用いて、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号化処理を実行し、コンテンツ鍵：Ｋｃを取り出す。さらに、取り出したコンテンツ鍵：Ｋｃを先の相互認証処理において生成したセッションキー（Ｋｓｅｓ）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【０２７１】（ｄ５）セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、［Ｋｓｅｓ（Ｋｃ）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０２７２】（ｄ６）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｄ７）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、（ｄ８）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｄ９）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０２７３】これらの処理によって、サービスプロバイダによる属性証明書（ＡＣ）に基づく利用期間の確認処理が行われ、制限された利用期間内である場合にのみ、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号可能な状態で再暗号化されて送付され、セキュリティチップにおいてコンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０２７４】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０２７５】（Ｂ）オンライン－利用回数制限コンテンツ

次に、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用回数が制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図３５のシーケンス図に従って説明する。

【０２７６】図３５に示す処理シーケンスは、先に説明した図３４の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０２７７】図３５に示す処理中、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ａ）、（ｂ）の各処理と、（ｃ）の相互認証処理は、図３４を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。（ｃ）の相互認証が成立すると、次に、図３５（ｄ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０２７８】（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オンライン回数制限である。

【０２７９】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンク

する公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０２８０】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、利用条件としてオンライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０２８１】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、属性証明書に格納された利用条件データ、利用制限回数を確認する。利用可能回数は、サービスプロバイダ内のデータベースに格納されており、サービスプロバイダでは、データベース内の管理データを参照して属性証明書に記録された回数制限内のコンテンツ利用であるか否かを判定する。

【０２８２】属性証明書に記録された回数制限内のコンテンツ利用であると判定されると、属性証明書中に格納されたコンテンツの復号に適用するコンテンツ鍵：Ｋｃの暗号化データ：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号を実行する。サービスプロバイダは、自己の所有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを用いて、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号化処理を実行し、コンテンツ鍵：Ｋｃを取り出す。

【０２８３】さらに、サービスプロバイダは、データベース内のコンテンツ利用回数管理データを更新し、利用対象コンテンツの対応する利用可能回数を１デクリメントする処理を行なう。さらに、サービスプロバイダでは、取り出したコンテンツ鍵：Ｋｃを先の相互認証処理において生成したセッションキー（Ｋｓｅｓ）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【０２８４】（ｄ５）セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、［Ｋｓｅｓ（Ｋｃ）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０２８５】（ｄ６）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｄ７）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、

（ｄ８）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｄ９）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０２８６】これらの処理によって、サービスプロバイダによる属性証明書（ＡＣ）に基づくコンテンツ利用回数の確認処理が行われ、制限された利用回数内である場合にのみ、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号可能な状態で再暗号化されて送付され、セキュリティチップにおいてコンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０２８７】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０２８８】（Ｃ）オフライン－買い切りコンテンツ

次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、買い切りコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図３６のシーケンス図に従って説明する。

【０２８９】図３６に示す処理シーケンスは、先に説明した図３４、図３５の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０２９０】図３６に示す処理中、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納され

ている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ａ）、（ｂ）の各処理は、図３４を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。（ａ）、（ｂ）のいずれかの処理によって、サービスプロバイダＩＤが取得されると、次に、図３６（ｃ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０２９１】（ｃ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オフライン買い切りである。

【０２９２】（ｃ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０２９３】（ｃ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップ制御部は、属性証明書内に格納された暗号化コンテンツ鍵：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを適用して復号化処理を実行し、コンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０２９４】（ｃ４）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｃ５）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、（ｃ６）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｃ７）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０２９５】これらの処理によって、属性証明書（ＡＣ）に基づく買い切りコンテンツであることの確認処理が行われ、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号され、コンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０２９６】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋを用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【０２９７】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０２９８】（Ｄ）オフライン－利用回数制限コンテンツ

次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数の制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理について説明する。属性証明書の利用条件がオフライン利用で、回数制限のあるコンテンツである場合、ユーザデバイス内で、属性証明書の設定条件に基づいて回数管理を実行するために、デバイス内にコンテンツ利用回数の管理データを持つことが必要となる。コンテンツ利用回数の管理データの保有処理が利用回数管理データのインポート処理である。

【０２９９】（Ｄ－１）インポート処理

まず、利用回数管理データのインポート処理について説明する。コンテンツ利用回数の管理態様には、コンテン

ツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する２つの態様がある。

【０３００】最初に図３７を参照して、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様とした場合の利用回数管理データのインポート処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。図３７の処理シーケンスは、すでにコンテンツ購入処理に伴うセキュリティチップと、サービスプロバイダ間の相互認証が成立し、サービスプロバイダからセキュリティチップに対する、購入コンテンツに対応する属性証明書の発行処理以降の処理を示している。ここで、サービスプロバイダの発行する属性証明書は、コンテンツ利用条件として、オフライン利用での利用回数制限コンテンツであることが記録され、コンテンツ利用制限回数が記録されている。

【０３０１】（１）属性証明書がサービスプロバイダから発行され、送信されると、（２）セキュリティチップの制御部は、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３０２】（３）セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証する。なお、ユーザがユーザデバイスにログインしている場合には、ユーザＩＤ等は保持されているので、ユーザＩＤ、サービスプロバイダＩＤはユーザが入力する代わりにユーザデバイスが送信してもよい。

【０３０３】セキュリティチップのメモリには、前述したように、登録されたサービスプロバイダ毎にサービスプロバイダ管理領域が設定され、その管理領域内にコンテンツ利用回数管理データが登録されることになる。図３８にセキュリティチップ内のメモリのサービスプロバイダ管理領域内に設定されるコンテンツ利用回数管理データの構成例を示す。

【０３０４】図３８に示すように、サービスプロバイダ管理領域には、サービスプロバイダＩＤ、ユーザＩＤ毎に、コンテンツ識別子としてのアプリケーションＩＤ（Ａｐｐ．ＩＤ＃ｎ）、対応する属性証明書（ＡＣ）の識別子であるＡＣシリアル（ＡＣ Ｓｅｒｉａｌ＃ｎ）、さらに残りの利用可能回数データ（Ｃｏｕｎｔ＃ｎ）が対応付けられて格納される。同一のコンテンツであっても利用ユーザ毎に異なる属性証明書に基づく利用回数カウントを可能としたデータ構成となっている。

【０３０５】図３７に戻って利用回数管理データのインポート処理のシーケンスについて説明を続ける。（３）セキュリティチップの制御部は、属性証明書から取得したコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データ、ユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証し、コンテンツ利用回数管理データが登録されていないことを確認すると、（４）コンテンツ利用回数管理データをサービスプロバイダ管理領域に追加登録し、（５）追加登録の終了後、属性証明書受信メッセージを生成して、サービスプロバイダに送信する。

【０３０６】図３７の例では、サービスプロバイダから受領した属性証明書（ＡＣ）は、
アプリケーションＩＤ：０００１
属性証明書（ＡＣ）シリアル：１３４５
コンテンツ利用制限回数：５
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３０７】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがメモリ内の対応するサービスプロバイダ管理領域にあるか否かを検証する。図３７に示すＳＰ管理領域データ（更新前）のデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５に対応するデータは存在しない。

【０３０８】従って、今回サービスプロバイダから受領した属性証明書に対応するコンテンツ利用回数管理デー

タをサービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、新たに追加する処理を行なう。その結果、図の下段に示すＳＰ管理領域データ（更新後）のデータ中に、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５の回数管理データが追加され、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：５が設定される。

【０３０９】コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を１デクリメントして、５→４→３→２→１→０とするデータ更新が実行され、利用可能回数が０となった以後のコンテンツ利用が拒否され、属性証明書に記録された利用制限回数内でのコンテンツ利用が可能となる。このコンテンツ利用処理については、後述する。

【０３１０】なお、サービスプロバイダから受領した属性証明書のアプリケーションＩＤ、属性証明書（ＡＣ）シリアルと同一のデータがすでに、対応するサービスプロバイダＩＤ、ユーザＩＤのサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして登録済みである場合には、重複した属性証明書の発行であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録は実行しない。

【０３１１】また、サービスプロバイダから受領した属性証明書のアプリケーションＩＤと同一であるが、属性証明書（ＡＣ）シリアルが異なるデータがすでに、対応するサービスプロバイダＩＤ、ユーザＩＤのサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして登録済みである場合には、異なる属性証明書に基づく同一コンテンツの新たな利用を可能とする属性証明書であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録を実行する。

【０３１２】すなわち、同一のサービスプロバイダＩＤ、同一ユーザＩＤのサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして、すでに、例えば
アプリケーションＩＤ：０００１、
ＡＣシリアル：０００１
残りコンテンツ利用回数：２
のデータが存在する場合であっても、

【０３１３】アプリケーションＩＤ：０００１
ＡＣシリアル：０００２
残りコンテンツ利用回数：５
の新たな管理データが追加登録される。

【０３１４】図３９に、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様とした場合のセキュリティチップ内で実行される利用回数管理データのインポート処理フローを示す。各ステップについて説明する。

【０３１５】まず、ステップＳ２２１において、属性証明書（検証済み）からアプリケーションＩＤ、利用制限回数、属性証明書シリアル番号を取り出す。ステップＳ２２２において、セキュリティチップ内のメモリに設定済みのサービスプロバイダ管理領域内に、属性証明書に格納されたと同一のアプリケーションＩＤの回数管理データがあるか否かを検索する。

【０３１６】ステップＳ２２３で、同一のアプリケーションＩＤの回数管理データの登録がないと判定された場合は、ステップＳ２２５に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データ登録を行なう。

【０３１７】一方、ステップＳ２２３において、同一のアプリケーションＩＤの回数管理データが登録済みと判定された場合は、ステップＳ２２４に進み、さらに、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがメモリ内のサービスプロバイダ管理領域に登録済みであるか否かを判定し、登録済みである場合は、同一の属性証明書に対する重複処理であると判定して、新たなデータ登録は実行せず処理を終了する。一方、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがメモリ内のサービスプロバイダ管理領域に登録済みでないと判定した場合は、ステップＳ２２５に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数データとして、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データの登録を行なう。

【０３１８】次に、図４０を参照して、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する処理態様とした場合の利用回数管理データのインポート処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。図４０の処理シーケンスは、すでにコンテンツ購入処理に伴うセキュリティチップと、サービスプロバイダ間の相互認証が成立し、サービスプロバイダからセキュリティチップに対する、購入コンテンツに対応する属性証明書の発行処理以降の処理を示している。ここで、サービスプロバイダの発行する属性証明書は、コンテンツ利用条件として、オフライン利用での利用回数制限コンテンツであることが記録され、コンテンツ利用制限回数が記録されている。

【０３１９】この処理態様は、セキュリティチップ内の限られたメモリ領域を有効に活用する構成であり、回数管理データの実データファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、この外部管理ファイル情報のハッシュ（Ｈａｓｈ）値

を、セキュリティチップ内部で管理することで、外部管理ファイル情報の改竄を検証することを可能としたものである。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣがハッシュ値となる。

【０３２０】図４０に示す処理シーケンスについて説明する。（１）属性証明書がサービスプロバイダから発行され、送信されると、（２）セキュリティチップの制御部は、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３２１】セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、外部のメモリからの回数管理ファイルの読み出し処理を実行する。図ではユーザデバイス制御部の管理するＨＤＤに回数管理ファイルがあり、（３）ユーザデバイス制御部において回数管理ファイルが読み出されてセキュリティチップに出力される。この読み出し対象は、管理ファイル全データであっても、あるいはコンテンツに対応するサービスプロバイダに関するデータのみであってもよい。

【０３２２】次に、セキュリティチップの制御部は、（４）ユーザデバイス制御部から受信した回数管理ファイルをセキュリティチップ内のＲＡＭに展開し、展開データに基づいてハッシュ値を計算する。回数管理データは、サービスプロバイダＩＤとユーザＩＤに対応付けられた複数の回数管理データを格納したフィールド構成を持つ。セキュリティチップのメモリ内のサービスプロバイダ管理領域には、サービスプロバイダＩＤとユーザＩＤに対応付けられたフィールドデータに対してハッシュ値が生成され格納されている。

【０３２３】セキュリティチップの制御部は、ユーザデバイス制御部から受信し、ＲＡＭに展開した回数管理ファイルから、ユーザにより指定されているサービスプロバイダＩＤ、ユーザＩＤに対応するフィールドデータを抽出してハッシュ値を計算し、計算された値と、セキュリティチップ内のメモリのサービスプロバイダ管理領域に格納されたハッシュ値とを比較する。算出ハッシュ値と、格納ハッシュ値が一致すれば、データに改竄がないと判定し、次の処理に進む。

【０３２４】図の例では、ＲＡＭ展開データの、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のフィールドデータに基づいてハッシュ値が算出され、セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールド、すなわち、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のハッシュ値：２９０ａと比較することになる。

【０３２５】（５）ハッシュ値が一致した場合は、一致した旨を示す通知をユーザデバイス制御部に送信し、一致が得られなかった場合はエラーメッセージをユーザデバイス制御部に送信する。（６）次に、セキュリティチップの制御部は、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、ユーザデバイス制御部から受信し、ＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。

【０３２６】コンテンツ利用回数管理データが登録されていないことを確認すると、（７）コンテンツの利用回数管理データを属性証明書（ＡＣ）から取り出し、ＲＡＭに展開した回数管理ファイルに追加登録し、（８）追加データに基づく新たなハッシュ値を計算して、（９）セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールドに格納する。（１０）追加登録の終了後、属性証明書受信メッセージを更新した回数管理ファイルとともに、ユーザデバイスに送信し、（１１）ユーザデバイスは、受信した回数管理ファイルをハードディスクに格納する。

【０３２７】図４０の例では、サービスプロバイダから受領した属性証明書（ＡＣ）は、
アプリケーションＩＤ：０００１
属性証明書（ＡＣ）シリアル：１３４５
コンテンツ利用制限回数：５
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３２８】セキュリティチップの制御部は、これらの

データに対応するコンテンツ利用回数管理データがＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。図４０に示す最上段のＳＣ内ＲＡＭのデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５に対応するデータは存在しない。

【０３２９】従って、今回サービスプロバイダから受領した属性証明書に対応するコンテンツ利用回数管理データをサービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、新たに追加する処理を行なう。その結果、図の中段に示すＳＣ内ＲＡＭのデータ中に、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５の回数管理データが追加され、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：５が設定される。

【０３３０】さらに、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するフィールドデータに基づいてハッシュ値が算出される。図の例では、データ更新前のハッシュ値は２９０ａであり、データ更新後のハッシュ値が８７３１であり、図の最下段のＳＰ管理領域のハッシュ値：８７３１が更新値として格納されることになる。

【０３３１】コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を１デクリメントして、５→４→３→２→１→０とするデータ更新が実行されるとともに、更新データに基づいて新たなハッシュ値が算出されて、更新処理が実行されることになる。このコンテンツ利用処理については、後述する。

【０３３２】なお、サービスプロバイダから受領した属性証明書のアプリケーションＩＤ、属性証明書（ＡＣ）シリアルと同一のデータがすでに、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルの対応するサービスプロバイダＩＤ、ユーザＩＤのフィールドのコンテンツ利用回数管理データとして登録済みである場合には、重複した属性証明書の発行であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録は実行しない。

【０３３３】また、サービスプロバイダから受領した属性証明書のアプリケーションＩＤと同一であるが、属性証明書（ＡＣ）シリアルが異なるデータがすでに、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルの対応するサービスプロバイダＩＤ、ユーザＩＤのフィールドのコンテンツ利用回数管理データとして登録済みである場合には、異なる属性証明書に基づく同一コンテンツの新たな利用を可能とする属性証明書であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録、ハッシュ値更新処理を実行する。

【０３３４】図４１に、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する処理態様とした場合の利用回数管理データのインポート処理フローを示す。各ステップについて説明する。

【０３３５】まず、ステップＳ２４１において、外部メモリから回数管理ファイルを読み込み、ステップＳ２４２において、サービスプロバイダＩＤ、ユーザＩＤに基づいて特定されるフィールドデータに基づくハッシュ値を算出し、算出ハッシュ値と、セキュリティチップのメモリ内のサービスプロバイダ管理領域に格納ずみのハッシュ値と一致するか否かを検証（Ｓ２４３）する。一致しない場合は、外部メモリから読み出した回数管理ファイルが改竄されていると判定し、エラー処理、例えばその後の処理を中止する。

【０３３６】ハッシュ値が一致し、外部メモリから読み出した回数管理ファイルが改竄されていないと判定した場合は、ステップＳ２４４に進み、属性証明書（検証済み）からアプリケーションＩＤ、利用制限回数、属性証明書シリアル番号を取り出す。次に、ステップＳ２４５において、ユーザデバイス制御部から受信し、ＲＡＭに展開した回数管理ファイルに、属性証明書に格納されたものと同一のアプリケーションＩＤの回数管理データがあるか否かを検索する。

【０３３７】ステップＳ２４６で、同一のアプリケーションＩＤの回数管理データの登録がないと判定された場合は、ステップＳ２４７に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データの登録を行なう。

【０３３８】一方、ステップＳ２４６において、同一のアプリケーションＩＤの回数管理データの登録が登録済みと判定された場合は、ステップＳ２５１に進み、さらに、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがＲＡＭに展開した回数管理ファイルに登録済みであるか否かを判定し、登録済みである場合は、同一の属性証明書に対する重複処理であると判定して、新たなデータ登録は実行せず処理を終了する。一方、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがＲＡＭに展開した回数管理ファイルに登録済みでないと判定した場合は、ステップＳ２４７に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データ登録を行なう。

【０３３９】ステップＳ２４７において、属性証明書に

従って、新たな回数管理データが、ＲＡＭに展開した回数管理ファイルに書き込まれると、ステップＳ２４８において、新規追加データを含めたデータに基づいて新たなハッシュ値が計算され、新たなハッシュ値をセキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールドに格納する。さらに、ステップＳ２４９において、更新した回数管理ファイルに基づいて外部メモリ（例えばハードディスク）に格納された回数管理ファイルの更新が実行される。

【０３４０】次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数制限コンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図４２のシーケンス図に従って説明する。

【０３４１】図４２に示す処理シーケンスは、先に説明した図３４、図３５、図３６の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０３４２】図４２に示す処理中、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ａ）、（ｂ）の各処理は、図３４を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。（ａ）、（ｂ）のいずれかの処理によって、サービスプロバイダＩＤが取得されると、次に、図４２（ｃ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０３４３】（ｃ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オフライン利用回数制限である。

【０３４４】（ｃ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３４５】（ｃ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップ制御部は、回数管理データの更新処理を実行する。回数管理データの更新処理の詳細については、後述する。さらに、セキュリティチップ制御部は、（ｃ４）属性証明書内に格納された暗号化コンテンツ鍵：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを適用して復号化処理を実行し、コンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０３４６】（ｃ５）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｃ６）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、（ｃ７）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｃ８）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０３４７】これらの処理によって、属性証明書（ＡＣ）に基づくコンテンツの利用回数制限内のコンテンツ利用である場合に限り、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号され、コンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０３４８】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋ

を用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【０３４９】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０３５０】次に、図４３、図４４を参照して、利用回数管理データの更新処理について説明する。コンテンツ利用可能回数の管理態様には、前述したようにコンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する２つの態様がある。図４３は前者、図４４は後者の態様における回数管理データの更新処理シーケンスを説明する図である。

【０３５１】最初に図４３を参照して、コンテンツ利用可能回をユーザデバイス内のセキュリティチップで管理する態様とした場合の回数管理データの更新処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。図４３の処理シーケンスは、すでにセキュリティチップ内で属性証明書の検証が済んでいるものとして、その後の処理を示している。

【０３５２】（１）セキュリティチップの制御部は、検証済みの属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証する。

【０３５３】セキュリティチップのメモリには、前述したように、登録されたサービスプロバイダ毎にサービスプロバイダ管理領域が設定され、その管理領域内にコンテンツ利用回数管理データが登録されることになる。

【０３５４】図４３に示す例では、属性証明書（ＡＣ）は、
アプリケーションＩＤ：０００２
属性証明書（ＡＣ）シリアル：３２７８
コンテンツ利用制限回数：１０
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３５５】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがメモリ内の対応するサービスプロバイダ管理領域にあるか否かを検証する。図４３に示すＳＰ管理領域データ（更新前）のデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータが存在し、利用可能回数（残回数）：７と設定されている。

【０３５６】（２）セキュリティチップ制御部は、この抽出データから利用可能回数（残回数）：７＞０であること、さらに、属性証明書に記録された制限回数以下、１０≧７であることを確認し、これらが確認されたことを条件としてコンテンツの利用を許可、すなわち、属性証明書に格納された（３）暗号化コンテンツ鍵の復号化処理を実行する。

【０３５７】（４）さらに、セキュリティチップ制御部は、メモリ内の対応するサービスプロバイダ管理領域の対応データの利用可能回数を１減少させるデータ更新処理を実行する。この場合は、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータ中の、利用可能回数（残回数）：７を６に更新する処理を実行する。なお、（３）の暗号化コンテンツ鍵の復号化処理と、（４）の回数管理データの更新処理は、処理手順を（４）を先に（３）を後にする構成としてもよく、また並列に実行してもよい。

【０３５８】次に、図４４を参照して、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する態様とした場合の回数管理データの更新処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。図４４の処理シーケンスは、すでにセキュリティチップ内で属性証明書の検証が済んでいるものとして、その後の処理を示している。

【０３５９】セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、外部のメモリからの回数管理ファイルの読み出し処理を実行する。図で

はユーザデバイス制御部の管理するＨＤＤに回数管理ファイルがあり、（１）ユーザデバイス制御部において回数管理ファイルが読み出されてセキュリティチップに出力される。この読み出し対象は、管理ファイル全データであっても、あるいはコンテンツに対応するサービスプロバイダに関するデータのみであってもよい。

【０３６０】次に、セキュリティチップの制御部は、（２）ユーザデバイス制御部から受信した回数管理ファイルをセキュリティチップ内のＲＡＭに展開し、展開データに基づいてハッシュ値を計算する。回数管理データは、サービスプロバイダＩＤとユーザＩＤに対応付けられた複数の回数管理データを格納したフィールド構成を持つ。セキュリティチップのメモリ内のサービスプロバイダ管理領域には、サービスプロバイダＩＤとユーザＩＤに対応付けられたフィールドデータに対してハッシュ値が生成され格納されている。

【０３６１】セキュリティチップの制御部は、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルから、ユーザにより指定されているサービスプロバイダＩＤ、ユーザＩＤに対応するフィールドデータを抽出してハッシュ値を計算し、計算された値と、セキュリティチップ内のメモリのサービスプロバイダ管理領域に格納されたハッシュ値とを比較する。算出ハッシュ値と、格納ハッシュ値が一致すれば、データに改竄がないと判定し、次の処理に進む。

【０３６２】図の例では、ＲＡＭ展開データの、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のフィールドデータに基づいてハッシュ値が算出され、セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールド、すなわち、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のハッシュ値：８７３１と比較することになる。

【０３６３】（３）ハッシュ値が一致した場合は、一致した旨を示す通知をユーザデバイスに送信し、一致が得られなかった場合はエラーメッセージをユーザデバイスに送信する。（４）次に、セキュリティチップの制御部は、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。

【０３６４】図４４に示す例では、属性証明書（ＡＣ）は、

アプリケーションＩＤ：０００２
属性証明書（ＡＣ）シリアル：３２７８
コンテンツ利用制限回数：１０
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３６５】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。図４４に示す最上段のＳＣ内ＲＡＭのデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータが存在し、利用可能回数（残回数）：７と設定されている。

【０３６６】（５）セキュリティチップ制御部は、この抽出データから利用可能回数（残回数）：７＞０であること、さらに、属性証明書に記録された制限回数以下、１０≧７であることを確認し、これらが確認されたことを条件としてコンテンツの利用を許可、すなわち、属性証明書に格納された（６）暗号化コンテンツ鍵の復号化処理を実行する。

【０３６７】（７）さらに、セキュリティチップ制御部は、ＲＡＭに展開した回数管理ファイルの対応データの利用可能回数を１減少させるデータ更新処理を実行する。この場合は、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータ中の、利用可能回数（残回数）：７を６に更新する処理を実行する。

【０３６８】さらに、セキュリティチップ制御部は、（８）更新データに基づく新たなハッシュ値を計算して、（９）セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールドに格納する。図４４の例では、更新前のアプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するフィールドデータに基づくハッシュ値は８７３１であり、更新後の同フィールドのデータに基づくハッシュ値はｂｃ３５となり、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応する図の最下段のＳＰ管理領域のハッシュ値：ｂｃ３５が更新ハッシュ値として格納されることになる。

【０３６９】（１０）更新処理の終了後、更新した回数管理ファイルを、ユーザデバイス制御部に送信し、ユーザデバイス制御部は、受信した回数管理ファイルをハードディスクに格納する。

【０３７０】このように、コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を１デクリメントして、５→４→３→２→１→０とするデータ更新が実行されるとともに、更新デ

ータに基づいて新たなハッシュ値が算出されて、更新処理が実行され、属性証明書に記録された利用制限回数内でのコンテンツ利用が可能となる。

【０３７１】以上、属性証明書のコンテンツ利用条件に従ったコンテンツの利用について説明した。なお、上記説明においては、期間制限と回数制限とを別々に説明したが、期間制限と回数制限の両制限を持つ属性証明書も可能であり、これらの場合は２つの条件に基づいてコンテンツ利用可否を判定した上で、属性証明書に設定された利用条件内の期限内、回数内のコンテンツ利用であることの確認を条件として、コンテンツ鍵の復号を行なうものとする。

【０３７２】［アップグレード処理］属性証明書には、コンテンツの利用条件として期間制限、回数制限、買い切り等の各種利用条件が設定され、これらの利用条件に基づいてセキュリティチップを持つユーザデバイスにおいてコンテンツの利用が行なわれることを説明した。次に、例えば属性証明書に設定されたコンテンツ利用制限回数の変更、あるいは期間制限の延長など、コンテンツの利用制限を変更する処理、すなわちアップグレード処理について説明する。

【０３７３】アップグレード処理には、具体的には、以下に説明する各種の態様がある。

（１）利用回数制限をコンテンツ利用条件として記録した属性証明書の利用可能回数を増やす。例えば、１０回券を買って、５回残っていて、１０回に増やす。１０回券を買って、使い切って、１０回券に増やす。

（２）利用期間制限をコンテンツ利用条件として記録した属性証明書の利用期間を延長する。例えば、１週間後までしか使えないものを、１ヶ月後まで使えるように期間を延長する。期間が切れて使えなくなったものを、１ヶ月後まで使えるように期間を延長する。

（３）回数制限や期間制限をコンテンツ利用条件として記録した属性証明書の利用条件の変更。例えば、回数制限を期間制限に変更する。期間制限を回数制限に変更する。回数制限を買い切りに変更する。期間制限を買い切りに変更する。

（４）アルバム化アップグレード一連のアルバム化されたコンテンツデータ、例えば１枚のＣＤあるいはＤＶＤ等に格納された複数（ｎ）のコンテンツ１～ｎ、あるいは何らかのシリーズ化されたコンテンツ１～ｎがあり、これらのいくつかを購入済であり、購入済みコンテンツに対応する属性証明書１～属性証明書ｎの複数をユーザがユーザデバイス内に保持している場合、例えば、コンテンツ１に対応する属性証明書１、コンテンツ３に対応する属性証明書３、コンテンツ５に対応する属性証明書５、をユーザデバイスに保持している場合、これらの属性証明書をサービスプロバイダに提示することにより、アルバムを構成する他のコンテンツ、すなわち、コンテンツ２，４，６～ｎのコンテンツを割引価格で一括（アルバム）購入できる。

【０３７４】属性証明書に基づくアップグレード処理には、上述した様々な態様がある。このアップグレード処理の実行シーケンスの概略は、次の通りである。まず、サービスプロバイダ（ＳＰ）がアップグレードメニューをユーザデバイスに提示し、ユーザがアップグレードメニューを選択する。ユーザデバイスは、ユーザの指定に従って、アップグレード処理対象とする取得済みの属性証明書の指定データとともに、アップグレード要求コマンドをセキュリティチップに送信する。セキュリティチップの制御部は、サービスプロバイダとの通信を実行して、アップグレード処理対象とする取得済みの属性証明書をサービスプロバイダに送信する。サービスプロバイダは、受信した属性証明書を検証した後、ユーザの指定したアップグレード処理を実行し、新たな属性証明書を発行しセキュリティチップに送信する。ユーザデバイスでは、新たな属性証明書の利用条件に従ってコンテンツを利用することが可能となる。

【０３７５】以下、アップグレードのベースとして用いる属性証明書（ＡＣ）に記載されたコンテンツ利用条件が以下の３態様である場合のアップグレード処理について、順次、説明する。

（Ａ）オンライン－利用期間制限コンテンツ
（Ｂ）オンライン－利用回数制限コンテンツ
（Ｃ）オフライン－利用回数制限コンテンツ

【０３７６】（Ａ）オンライン－利用期間制限属性証明書（ＡＣ）をベースとしたアップグレード処理

まず、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用期間制限が設定された属性証明書を保有する場合、このオンライン－利用期間制限属性証明書をベースとしたアップグレード処理を図４５のシーケンス図に従って説明する。図４５には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０３７７】図４５では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ｃ）の相互認証処理、（ｄ）のコンテンツ取得処理は共通に実行される。

【０３７８】まず、（ａ）の処理から説明する。（ａ１）ユーザデバイス制御部は、アップグレード処理対象の属性証明書の検索をセキュリティチップ制御部に要求する。（ａ２）セキュリティチップ制御部は、チップのメモリに格納済みの属性証明書のリストをユーザデバイ

ス制御部に出力し、（ａ３）ユーザデバイスでは付属のブラウザによりリストを表示する。（ａ４）ユーザは表示されたリストからアップグレード処理対象の属性証明書（ＡＣ）を指定し、読み出し命令をセキュリティチップ制御部に送信する。（ａ５）セキュリティチップ制御部は、指定された属性証明書を内部メモリから読み出してユーザデバイス制御部に出力し、（ａ６）ユーザデバイスでは付属のブラウザにより属性証明書を表示し、属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０３７９】属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合は、（ｂ）の処理となる。（ｂ１）ユーザデバイス制御部は、アップグレード処理対象の属性証明書の検索を実行し、（ｂ２）ユーザデバイスでは付属のブラウザにより表示されたＡＣリストからアップグレード処理対象の属性証明書（ＡＣ）を指定し、読み出して属性証明書を表示し、（ｂ４）属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０３８０】上記（ａ）、（ｂ）のいずれかの処理によって取得されたサービスプロバイダ識別子（ＳＰ　ＩＤ）は、サービスプロバイダ管理領域から、相互認証に必要な情報を取得するために用いられる。前述したように、サービスプロバイダ管理領域へのアクセスにはサービスプロバイダ毎に設定されたパスワード入力が必要であり、ユーザは、属性証明書から取得したサービスプロバイダ識別子（ＳＰ　ＩＤ）に対応するパスワード入力により、サービスプロバイダ管理領域へのアクセスを実行し、図４５の（ｃ１）に示すセキュリティチップとサービスプロバイダ間の相互認証処理を実行する。

【０３８１】この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。相互認証が成立すると、次に、図４５（ｄ）に示す処理、すなわちアップグレード属性証明書取得処理を実行する。

【０３８２】（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オンライン期間制限であり、ユーザの指定するアップグレード条件は、例えば、

期間制限の変更（延長）

期間制限→オンライン回数制限へ変更

期間制限→オフライン回数制限へ変更

期間制限→買い切りへ変更

等の条件である。

【０３８３】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。

【０３８４】さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３８５】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオンライン期間制限コンテンツであることが記録され、また有効期限データが格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０３８６】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０３８７】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレ

ードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０３８８】なお、アップグレードの態様は、前述したように、

期間制限の変更（延長）

期間制限→オンライン回数制限へ変更

期間制限→オフライン回数制限へ変更

期間制限→買い切りへ変更

のいずれかであり、期間制限の変更の場合は、利用期間を新たに設定したアップグレード属性証明書を生成する。また、オンラインまたはオフライン回数制限へ変更する場合は、利用制限回数を格納したアップグレード属性証明書を生成する。また、買い切りへ変更する場合は、コンテンツ利用条件を買い切りとしたアップグレード属性証明書を生成する。

【０３８９】期間制限の変更、あるいはオンライン回数制限へ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］として格納するが、オフライン回数制限へ変更、または買い切りへ変更する場合は、アップグレード属性証明書には、元の属性証明書とは異なり、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納する。

【０３９０】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図４５のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０３９１】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０３９２】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０３９３】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレード属性証明書をメモリに格納する。

【０３９４】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データのインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０３９５】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレード属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０３９６】（Ｂ）オンライン－利用回数制限属性証明書（ＡＣ）をベースとしたアップグレード処理

次に、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用回数制限が設定された属性証明書を保有する場合、このオンライン－利用回数制限属性証明書をベースとしたアップグレード処理を図４６のシーケンス図に従って説明する。図４６には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０３９７】図４６では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、（ｃ）はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図４５の場合と同様であり、説明を省略する。

【０３９８】相互認証後成立後の処理から説明する。

（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オンライン回数制限であり、ユーザの指定するアップグレード条

件は、例えば、
利用可能回数の変更（回数増加）
オンライン回数制限→期間制限へ変更
オンライン回数制限→オフライン回数制限へ変更
オンライン回数制限→買い切りへ変更
等の条件である。

【０３９９】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４００】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオンライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０４０１】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０４０２】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０４０３】なお、アップグレードの態様は、前述したように、
利用制限回数の変更（回数増加）
オンライン回数制限→期間制限へ変更
オンライン回数制限→オフライン回数制限へ変更
オンライン回数制限→買い切りへ変更
のいずれかであり、回数制限の変更の場合は、利用制限回数を新たに設定したアップグレード属性証明書を生成する。また、期間制限へ変更する場合は、期間制限情報を格納したアップグレード属性証明書を生成する。

【０４０４】オンライン回数制限として利用制限回数を変更する場合、期間制限へ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］として格納するが、オフライン回数制限へ変更、または買い切りへ変更する場合は、アップグレード属性証明書には、元の属性証明書とは異なり、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納する。

【０４０５】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図４６のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０４０６】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０４０７】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０４０８】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレ

ード属性証明書をメモリに格納する。

【０４０９】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０４１０】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレード属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０４１１】（Ｃ）オフライン－利用回数制限属性証明書（ＡＣ）をベースとしたアップグレード処理

次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数制限が設定された属性証明書を保有する場合、このオフライン－利用回数制限属性証明書をベースとしたアップグレード処理を図４７のシーケンス図に従って説明する。図４７には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０４１２】図４７では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、（ｃ）はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図４５の場合と同様であり、説明を省略する。

【０４１３】相互認証後成立後の処理から説明する。

（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オフライン回数制限であり、ユーザの指定するアップグレード条件は、例えば、

利用可能回数の変更（回数増加）

オフライン回数制限→期間制限へ変更

オフライン回数制限→オンライン回数制限へ変更

オフライン回数制限→買い切りへ変更等の条件である。

【０４１４】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４１５】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオフライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］が格納されている。

【０４１６】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０４１７】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０４１８】なお、アップグレードの態様は、前述したように、

利用制限回数の変更（回数増加）

オフライン回数制限→期間制限へ変更

オフライン回数制限→オンライン回数制限へ変更

オフライン回数制限→買い切りへ変更

のいずれかであり、回数制限の変更の場合は、利用制限回数を新たに設定したアップグレード属性証明書を生成する。また、期間制限へ変更する場合は、期間制限情報

を格納したアップグレード属性証明書を生成する。

【０４１９】オフライン回数制限として利用制限回数を変更する場合、買い切りへ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］として格納するが、期間制限へ変更、またはオンライン回数制限へ変更する場合は、元の属性証明書とは異なり、アップグレード属性証明書に格納するコンテンツ鍵は、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］とする。

【０４２０】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図４７のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０４２１】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０４２２】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０４２３】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレード属性証明書をメモリに格納する。

【０４２４】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０４２５】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレード属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０４２６】（Ｄ）アルバム購入型アップグレード

次に、一連のアルバム化されたコンテンツデータ、例えば１枚のＣＤあるいはＤＶＤ等に格納された複数（ｎ）のコンテンツ１～ｎ、あるいは何らかのシリーズ化されたコンテンツ１～ｎがあり、これらのいくつかを購入済であり、購入済みコンテンツに対応する属性証明書１～属性証明書ｎの複数をユーザがユーザデバイス内に保持している場合、これらの属性証明書をサービスプロバイダに提示することにより、アルバムを構成する他のコンテンツ、すなわち、コンテンツ２，４，６～ｎのコンテンツを割引価格で一括（アルバム）購入する処理としたアップグレード処理について、図４８を参照して説明する。

【０４２７】図４８は、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、（ｃ）はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図４５の場合と同様であり、説明を省略する。

【０４２８】相互認証後成立後の処理から説明する。

（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書は、ある複数のコンテンツの集合対として識別されるアルバムを構成する一部のコンテンツに対応する１以上の属性証明書である。ユーザの指定するアップグレード条件は、例えば、

アルバムを構成する他の一部コンテンツの購入

アルバムを構成する他の全コンテンツの購入等の条件である。

【０４２９】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を

実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４３０】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。

【０４３１】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０４３２】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０４３３】なお、アップグレードの態様は、前述したように、

アルバムを構成する他の一部コンテンツの購入

アルバムを構成する他の全コンテンツの購入

のいずれかであり、アルバムを構成する他の一部コンテンツの購入の場合は、購入指定の一部コンテンツに対応するアップグレード属性証明書を生成する。また、アルバムを構成する他の全コンテンツの購入の場合は、アルバムを構成する他の全コンテンツに対応するアップグレード属性証明書を生成する。

【０４３４】なお、この場合の利用条件は、ユーザが予め指定することも可能であり、また、サービスプロバイダが決定する構成としてもよい。ユーザが指定する場合は、図４８のステップ（ｄ１）において指定し、（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、指定条件を併せて送付する。

【０４３５】サービスプロバイダは、オフライン利用とするアップグレード属性証明書を生成する場合は、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納し、オンライン利用とするアップグレード属性証明書を生成する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］とする。

【０４３６】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図４８のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０４３７】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０４３８】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０４３９】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレード属性証明書をメモリに格納する。

【０４４０】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０４４１】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレー

ド属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０４４２】［データバックアップおよびリストア処理］ユーザがサービスプロバイダから購入し、セキュリティチップを有するユーザデバイス内の記憶手段に格納した権利情報や、証明書類は、消失の事態に備えてバックアップしておくことが好ましい。バックアップすべき情報には、見られてもいい情報と、セキュアに保持しなければいけない情報がある。見られてもいい情報とは、公開鍵証明書、属性証明書などの証明書類である。セキュアに保持する情報とは、例えばセキュリティチップのサービスプロバイダ管理領域に書き込まれているサービス加入の証拠情報などがある。

【０４４３】公開鍵証明書、属性証明書などの証明書類については、ユーザが適宜、ハードディスクやフラッシュメモリを搭載したメモリカードなどに複製情報を格納しておくことで十分である。属性証明書にはコンテンツ鍵が格納されているが、オンライン利用の場合には、サービスプロバイダとの接続が必要となり、この際の相互認証時にデバイス（セキュリティチップ）の正当性が確認されるので、コンテンツが不正に利用されることはない。また、オフライン利用の場合でも、コンテンツ鍵を復号するための鍵は、セキュリティチップのサービスプロバイダ管理領域に格納されているので、正当なユーザデバイスのセキュリティチップを保持し、かつ前述したパスワードによるアクセスが許可されたユーザのみが暗号化コンテンツ鍵を復号することが可能となる。従って、属性証明書が第三者に渡ったとしてもコンテンツの不正利用が発生することはない。

【０４４４】しかし、セキュリティチップ内の秘密情報に関しては、テンポラリのストレージにセキュアに保持しておかねばならない。例えばセキュリティチップのサービスプロバイダ管理領域には、サービスプロバイダとの相互認証に必要なＩＤ情報、鍵情報、パスワード等が格納されており、これらは第三者に漏洩することを防止することが必要である。従って外部の記憶媒体（テンポラリのストレージ）にバックアップする際には、これらのバックアップデータは、暗号化しておくことが必要である。

【０４４５】ユーザが秘密情報をテンポラリのストレージに格納した場合、ストレージメディアの盗難によりデータ漏洩が発生する暗号化では意味がない。また、ユーザデバイスから容易に取り出せる鍵によって復号できる構成とすると、ユーザデバイスから取り出した鍵によって、セキュリティデバイスの複製を生成することが可能となってしまい、ユーザサイドで全く同様のサービスプロバイダ管理領域データを有する第２のセキュリティデバイスを生成することが可能となるおそれがある。また、複製したセキュリティチップを搭載した可搬メディアを他のユーザデバイスに装着することで、複数のユーザデバイスで全く同様のサービスを受けることが可能となってしまう。そこで本発明のシステムでは、テンポラリのストレージに秘密情報をバックアップデータとして格納した場合でも、不正な第三者によって復号できない態様とするとともに、ユーザデバイスを保持するユーザ自身もシステムホルダの許可なくリストア等、他のセキュリティチップに格納して使用することのできない構成とし、データの復号、リストアはサポートセンタにおいてのみ実行可能とした。

【０４４６】すなわち、ユーザデバイス内で確実な情報管理を実行し、データ消失を完全に防ぐことの困難性に鑑み、本発明のシステムにおいては、サポートセンタにおいて、データのバックアップ・サービスを提供し、必要に応じてサポートセンタにおいて、バックアップデータを用いてデータ復旧、すなわちリストア処理を実行する。リストアは、サポートセンターにて行い、テンポラリのストレージからデータを読み出し、ユーザデバイスのセキュリティデバイスに対してインポートする処理として実行する。以下、サポートセンタによるデータバックアップ処理、およびリストア処理について説明する。

【０４４７】図４９に、ユーザデバイス内の秘密情報のバックアップ処理、サポートセンタにおけるリストア処理の概要を説明する図を示す。

【０４４８】図４９において、ユーザデバイス４１０は、セキュリティチップ４１１を有し、セキュリティチップには様々なシークレット、すなわち秘密情報が格納されている。秘密情報は、例えばセキュリティチップのサービスプロバイダ管理領域の格納情報であり、サービスプロバイダとの相互認証に必要なＩＤ情報、鍵情報、パスワード等である。また、ユーザデバイスのセキュリティチップ外のメモリには、公開鍵証明書、属性証明書が格納される。

【０４４９】ユーザは、ユーザデバイスの損壊、あるいはデータの消失等に備え、これらの情報をユーザデバイス以外の外部の記憶媒体にバックアップして保存する。例えば公開鍵証明書、属性証明書等を外部のＰＣのハードディスクに格納したり、フラッシュメモリを備えたカード型記憶媒体などの外部記憶媒体４２１に格納する。これらは、前述したように、漏洩により、コンテンツの不正利用を発生させるおそれがなく、暗号化されることなく外部の記憶媒体４２１に格納し、必要に応じてユーザが記憶媒体４２１からユーザデバイス４１０にリストアすることが可能である。

【０４５０】一方、セキュリティチップに格納された秘密情報は、外部の記憶媒体４２２にバックアップデータとして保存する場合は、ユーザデバイスにおいて一時的な鍵として乱数からバックアップ鍵：Ｋｂ（共通鍵系）を生成し、バックアップ鍵：Ｋｂによって、各種の秘密情報（ＳｅｃＤａｔａ）を暗号化し、暗号化データ：

［Ｋｂ（ＳｅｃＤａｔａ）］として記憶媒体４２２に格納する。さらに、生成したバックアップ鍵：Ｋｂをサポートセンタの公開鍵：Ｋｐｓによって暗号化した暗号鍵データ［Ｋｐｓ（Ｋｂ）］を併せて外部記憶媒体４２２に格納する。秘密情報を外部の記憶媒体４２２に格納した後、バックアップ鍵：Ｋｂはユーザデバイスに保持することなく消去する。

【０４５１】記憶媒体４２２に格納した暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］は、たとえ記憶媒体４２２が第三者の手に渡ったとしても、その復号のための鍵であるバックアップ鍵：Ｋｂが、サポートセンタの公開鍵：Ｋｐｓによって暗号化されており、バックアップ鍵：Ｋｂを取得するためには、サポートセンタの秘密鍵：Ｋｓｓによる復号化処理が必要となるので、第三者による復号は不可能である。また、ユーザデバイスを保持する正当なユーザも復号により第２のセキュリティデバイスを生成することはできない。

【０４５２】データのリストア（復旧）処理は、ユーザサイト側からサポートセンタ４５０に対して記憶媒体４２２を送付することによって実行される。リストア処理は、元のユーザデバイスが損壊した場合は、新たなユーザデバイス４３０に対して実行される。元のユーザデバイス自体をサポートセンタに送付して、修理された元のユーザデバイスに対してリストアを実行することも可能である。なお、新たなユーザデバイスに対するリストア処理を実行する場合は、元のユーザデバイスを無効化する処理、すなわちリボーク処理を併せて実行する。このリボーク処理は、例えばユーザデバイスに対応して発行されている公開鍵証明書をリボケーションリストに登録することによって行われる。リボケーションリストは、不正デバイス、無効化されたデバイス、ユーザ等に対応する公開鍵証明書のリストとして構成されるものである。リボケーションリストは、デバイスとの相互認証時に参照され、リストに記載されたデバイスであると判定されると認証を不成立として、その後のデータ通信を中止することを可能としたものである。

【０４５３】サポートセンタ４５０におけるリストア処理は、まず、ユーザサイトから送付された記憶媒体４２２’に格納されたサポートセンタの公開鍵：Ｋｐｓによって暗号化した暗号鍵データ［Ｋｐｓ（Ｋｂ）］を取り出して、サポートセンタの秘密鍵：Ｋｓｓによって復号してバックアップ鍵:Ｋｂを取り出す。その後、取得したバックアップ鍵:Ｋｂを適用して、バックアップ鍵により暗号化された秘密情報暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］の復号化処理を実行し、復号データ：ＳｅｃＤａｔａをユーザデバイス４３０のセキュリティチップ内に格納する処理として実行される。具体的なリストア処理シーケンスについては、後述する。

【０４５４】上述したように、ユーザデバイス内の秘密情報のバックアップデータのリストアをサポートセンタのみにおいて実行可能とした構成により、秘密情報の複製利用を防止することが可能となる。

【０４５５】図５０にリストア処理時の手順概要を説明する図を示す。ユーザサイトでは、ユーザが使用しているユーザデバイス４７０内のセキュリティチップに格納された秘密情報をバックアップストレージメディア４７１に格納する。前述したように、ユーザデバイスは、バックアップ鍵：Ｋｂ（共通鍵系）を生成し、バックアップ鍵：Ｋｂによって秘密情報（ＳｅｃＤａｔａ）を暗号化したデータ：［Ｋｂ（ＳｅｃＤａｔａ）］と、バックアップ鍵：Ｋｂをサポートセンタの公開鍵：Ｋｐｓによって暗号化した暗号鍵データ［Ｋｐｓ（Ｋｂ）］をバックアップストレージメディア４７１に格納する。

【０４５６】ユーザデバイス４７０が損壊する等の理由により、使用できなくなった場合、ユーザは、バックアップストレージメディア４７１をサポートセンタ４７５に送付する。

【０４５７】サポートセンタ４７５は、新規のユーザデバイス、あるいは損壊したユーザデバイスを修理した元のユーザデバイスに対して、バックアップストレージメディア４７１のデータを復号してリストアし、秘密情報をリストアしたユーザデバイス４７２と、リストアに使用したバックアップストレージメディア４７１をユーザに返却する。サポートセンタ４７５は、このリストア処理において、新規デバイスに対してリストア処理を実行し、元のデバイスを使用しない場合には、前述したリボーケーションリストへの登録によるリボーク処理を実行する。またサポートセンタ４７５は、リストア処理に対する課金を実行してもよい。

【０４５８】図５１を参照して、ユーザサイトで実行するバックアップストレージメディアに対するデータバックアップ処理シーケンスについて説明する。図５１は、左からバックアップストレージメディア、ユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。まず、（１）ユーザデバイス制御部は、セキュリティチップ制御部に対してバックアップ処理要求を送信する。これは、ユーザがユーザデバイス側の入力部に対するユーザによるバックアップ処理実行指示に基づいて行われる。

【０４５９】セキュリティチップの制御部は、バックアップ要求を受信すると、（２）バックアップデータの暗号化に適用するバックアップ鍵（キー）：Ｋｂを生成する。バックアップ鍵（キー）：Ｋｂは例えば乱数生成手段によって生成した乱数に基づいて生成するバックアップ専用の一時的な鍵であり、バックアップストレージメディアに対するバックアップ処理の後、セキュリティチップに保持されることなく、消去される。

【０４６０】セキュリティチップの制御部は、（３）バックアップ鍵（キー）：Ｋｂの生成後、生成したバックアップ鍵（キー）で、バックアップデータの暗号化を行

ない、暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］を生成する。データ暗号化が終了すると、さらに、（４）セキュリティチップの制御部は、バックアップ鍵（キー）：Ｋｂをサポートセンタの公開鍵：Ｋｐｓを用いて暗号化して暗号鍵データ：［Ｋｐｓ（Ｋｂ）］を生成する。

【０４６１】上記処理の後、セキュリティチップの制御部は、（５）暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］と、暗号鍵データ：［Ｋｐｓ（Ｋｂ）］をバックアップストレージメディアに格納する。なお、これらの処理の後、バックアップ鍵（キー）：Ｋｂは、セキュリティチップから消去される。

【０４６２】なお、バックアップストレージメディアに暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］と、暗号鍵データ：［Ｋｐｓ（Ｋｂ）］を格納することなく、これらのデータを直接サポートセンタに送信し、サポートセンタ内の記憶手段にユーザデバイスＩＤ、またはセキュリティチップＩＤに対応させてバックアップデータを保存する構成としてもよい。このような構成とした場合は、バックアップデータに基づくリストア処理は、ユーザデバイス（セキュリティチップ）側からサポートセンタに対する通信ネットワークを介したリクエストに応じて実行可能となり、バックアップストレージメディアを送付することなく、リストア処理を実行することが可能となる。

【０４６３】次に、図５２を参照して、サポートセンタで実行するバックアップストレージメディアからのバックアップデータの取得処理について説明する。サポートセンタでは、まず、ユーザサイトから送付されたバックアップストレージメデイアに格納されたデータを読み出す。読み出しデータは、バックアップ鍵（キー）：Ｋｂで暗号化されたバックアップデータ：［Ｋｂ（ＳｅｃＤａｔａ）］と、バックアップ鍵（キー）：Ｋｂをサポートセンタの公開鍵：Ｋｐｓを用いて暗号化した暗号鍵データ：［Ｋｐｓ（Ｋｂ）］である。なお、前述したように、サポートセンタ内の記憶手段にユーザデバイスＩＤ、またはセキュリティチップＩＤに対応させてバックアップデータを保存した構成とした場合は、サポートセンタは、ユーザサイトからのリストア処理リクエストに基づいて、記憶手段からこれらのデータの読み出しを行なう。

【０４６４】サポートセンタは、データの読み出しの後、まずサポートセンタの公開鍵：Ｋｐｓで暗号化したバックアップ鍵（キー）：Ｋｂデータ：［Ｋｐｓ（Ｋｂ）］を、サポートセンタの公開鍵に対応する秘密鍵：Ｋｓｓで復号化処理を実行し、バックアップ鍵（キー）：Ｋｂを取り出す。さらに、バックアップ鍵（キー）：Ｋｂで暗号化されたバックアップデータ：［Ｋｂ（ＳｅｃＤａｔａ）］を、取り出したバックアップ鍵（キー）：Ｋｂを適用して復号化処理を実行し、バックアップデータ：ＳｅｃＤａｔａを取り出す。

【０４６５】次に、図５３を参照して、サポートセンタで実行するリストア処理のシーケンスについて説明する。図５３は、左から、リストア処理によりデータを格納する新たなユーザデバイスのセキュリティチップ制御部、およびユーザデバイス制御部、サポートセンタサーバ、さらに、属性証明書発行者である属性証明書認証局（ＡＡ：Attribute Certificate Authority）の処理を示している。なお、属性証明書発行局は、属性証明書を発行する機関であり、例えばサービスプロバイダ内に構成される。ここで属性証明書発行局は、ユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ管理領域を生成するための属性証明書である。

【０４６６】前述したように、サービスプロバイダ管理領域生成用の属性証明書は、サービスプロバイダがユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ毎の管理領域を登録設定することを目的として発行される属性証明書であり、属性情報フィールドには、サービスプロバイダ識別子（ＩＤ）、サービスプロバイダ・ネーム、処理態様：メモリ領域確保、領域サイズ：メモリ領域のサイズ等が記録される。

【０４６７】図５３の処理シーケンスについて説明する。まず、（１）ユーザデバイス制御部からセキュリティチップ制御部に対してリストア処理要求が出力される。これは、サポートセンタのオペーレータによってユーザデバイス側の入力部に対して実行するリストア処理実行指示に基づいて行われる。

【０４６８】セキュリティチップ制御部は、（２）ユーザデバイス制御部からリストア処理要求を受信すると、（３）セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サポートセンタはセッション鍵（Ｋｓｅｓ）を共有する。相互認証が成立すると、次に、（４）セキュリティチップ制御部は、サポートセンタに対してリストア処理要求を送信する。

【０４６９】サポートセンタは、セキュリティチップからのリストア処理要求を受信すると、（５）バックアップデータの検索処理を行なう。これは、サポートセンタが、ユーザサイトからバックアップデータを受領済みであるか否かの確認として実行される。

【０４７０】サポートセンタは、次に、（６）メモリ領域確保用属性証明書（ＡＣ）の発行要求を属性証明書発行局（者である）に対して送信する。（７）属性証明書（ＡＣ）の発行要求を受信した属性証明書発行者である属性証明書認証局（ＡＡ）は、メモリ領域確保用属性証

明書（ＡＣ）を生成する。なお、属性証明書（ＡＣ）は、予め属性証明書認証局（ＡＡ）から発行を受けておいてもよい。

【０４７１】メモリ領域確保用属性証明書は、属性情報フィールドに、サービスプロバイダ識別子（ＩＤ）、サービスプロバイダ・ネーム、処理態様：メモリ領域確保、領域サイズ：メモリ領域のサイズ等が記録されたものであり、例えば各サービスプロバイダの管理の下に発行される。従って、リストア処理が１つのサービスプロバイダ管理領域内のデータについてのみ実行される場合は、１つのメモリ領域確保用属性証明書によりセキュリティチップ制御部内のメモリに１つのサービスプロバイダ管理領域が設定され、データのリストアが実行されるが、複数のサービスプロバイダ管理領域内のデータについてリストアを実行する場合は、複数のメモリ領域確保用属性証明書の発行を受けて、セキュリティチップ制御部内のメモリに複数のサービスプロバイダ管理領域を設定した上で、各利用域についてデータ格納を行なうことになる。

【０４７２】（８）属性証明書発行者である属性証明書認証局（ＡＡ）は、生成したメモリ領域確保用属性証明書（ＡＣ）をサポートセンタサーバに送信する。サポートセンタは、属性証明書発行者である属性証明書認証局（ＡＡ）からメモリ領域確保用属性証明書（ＡＣ）を受信すると、（９）属性証明書、およびバックアップデータをセキュリティチップ制御部に送信する。バックアップデータは、メモリ領域確保用属性証明書（ＡＣ）によって、セキュリティチップのメモリに確保されるサービスプロバイダ管理領域に格納するデータであり、例えば、サービスプロバイダ（ＳＰ）対応秘密鍵、サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵、外部管理情報のハッシュ値、利用回数管理データ、認証情報、ユーザ情報等の各データである。

【０４７３】（１０）セキュリティチップ制御部は、サポートセンタサーバからのメモリ領域確保用属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。

【０４７４】さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４７５】（１１）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、メモリ領域確保用属性証明書（ＡＣ）に記録された条件に従って、セキュリティチップ内のメモリにサービスプロバイダ管理領域を設定する。（１２）さらに、セキュリティチップの制御部は、メモリに設定されたサービスプロバイダ管理領域内にサポートセンタサーバから受信したバックアップデータを格納する。

【０４７６】以上の処理により、ユーザデバイスのセキュリティチップのメモリに、メモリ領域確保用属性証明書に記録された条件に従ってサービスプロバイダ管理領域が確保され、確保されたサービスプロバイダ管理領域にバックアップデータが格納される。なお、複数のサービスプロバイダ管理領域に対応するバックアップデータのリストアを行なう場合は、複数のメモリ領域確保用属性証明書の発行に基づいて同様の処理を繰り返し実行する。

【０４７７】なお、上述の処理シーケンスの後、あるいはその途中において、サポートセンタは、廃棄対象となる元のユーザデバイスのリボーク処理を実行する。さらに、リストアを要求してきたユーザに対する課金処理を実行してもよい。

【０４７８】［各エンティテイの構成］次に、上述したコンテンツ利用管理システムを構成する各エンティテイの構成例について図を参照しながら、説明する。まずサービスプロバイダからのコンテンツを受領するサービス受領デバイスとしてのユーザデバイスの構成例を図５４を参照して説明する。

【０４７９】ユーザデバイスはデータ処理、制御を実行するＣＰＵ、サービスプロバイダ他と通信可能な通信手段を備えたＰＣ等のデータ処理手段によって実現することができる。図５４にデバイスの構成例を示す。なお、図５４に示すデバイス構成例は１つの例であり、デバイスは、ここに示すべての機能を必ずしも備えることが要求されるものではない。図５４に示すＣＰＵ(Central processing Unit)５０１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実行するプロセッサである。ＲＯＭ（Read-Only-Memory）５０２は、ＣＰＵ５０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）５０３は、ＣＰＵ５０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【０４８０】ＨＤＤ５０４はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。セキュリティチップ５１２は、前述したように耐タンパ構造を持つ

構成であり、暗号処理に必要な鍵データ、アクセス許可書の格納領域としてのメモリ、制御部を有する。

【０４８１】バス５１０はＰＣＩ（Peripheral Component Interface）バス等により構成され、各モジュール、入出力インタフェース５１１を介した各入手力装置とのデータ転送を可能にしている。

【０４８２】入力部５０５は、例えばキーボード、ポインティングデバイス等によって構成され、ＣＰＵ５０１に各種のコマンド、データを入力するためにユーザにより操作される。出力部５０６は、例えばＣＲＴ、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

【０４８３】通信部５０７はデバイスの接続したエンティテイ、例えばサービスプロバイダ等との通信処理を実行し、ＣＰＵ５０１の制御の下に、各記憶部から供給されたデータ、あるいはＣＰＵ５０１によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティテイからのデータを受信する処理を実行する。

【０４８４】ドライブ５０８は、フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体５０９の記録再生を実行するドライブであり、各リムーバブル記録媒体５０９からのプログラムまたはデータ再生、リムーバブル記録媒体５０９に対するプログラムまたはデータ格納を実行する。

【０４８５】各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ５０１において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース５１１、バス５１０を介して例えば接続されているＲＡＭ５０３に供給される。

【０４８６】前述の説明内に含まれるユーザデバイスにおける処理を実行するためのプログラムは例えばＲＯＭ５０２に格納されてＣＰＵ５０１によって処理されるか、あるいはハードディスクに格納されＨＤＤ５０４を介してＣＰＵ５０１に供給されて実行される。

【０４８７】次に、本発明のシステムの構成エンティテイであるサービスプロバイダ、サポートセンタ、コンテンツクリエータ、属性証明書発行局等の各エンティテイを構成するデータ処理装置の構成例について説明する。これらのエンティテイは例えば図５５に構成によって実現することができる。なお、図５５に示すデータ処理装置構成例は１つの例であり、各エンティテイは、ここに示すべての機能を必ずしも備えることが要求されるものではない。

【０４８８】図５５に示すＣＰＵ(Central processing Unit)６０１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実際に実行する。ＲＯＭ（Read-Only-Memory）６０２は、ＣＰＵ６０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）６０３は、ＣＰＵ６０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。ＨＤＤ６０４はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。暗号処理手段６０５は、送信データの暗号処理、復号化処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをＲＯＭ６０２に格納し、ＣＰＵ６０１がＲＯＭ格納プログラムを読み出して実行するように構成してもよい。

【０４８９】ドライブ６０６は、フロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体６０７の記録再生を実行するドライブであり、各リムーバブル記録媒体６０７からのプログラムまたはデータ再生、リムーバブル記録媒体６０７に対するプログラムまたはデータ格納を実行する。各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ６０１において実行または処理を行なう場合は、読み出したプログラム、データはバス６１０を介して例えば接続されているＲＡＭ６０３、通信部６０８、通信部６０９に供給される。

【０４９０】通信部６０８、通信部６０９は、それぞれ異なるエンティテイを通信相手として通信する処理を想定して複数の通信部を設けた例を示している。例えばサービスプロバイダであれば、一方はユーザデバイスとの通信、他方はコンテンツクリエータとの通信処理に使用される。各通信部を介して通信相手との相互認証、暗号化データの送受信処理等が実行される。

【０４９１】前述した説明内に含まれるサービスプロバイダ、サポートセンタ、コンテンツクリエータ、属性証明書発行局を構成するデータ処理装置における各処理を実行するためのプログラムは例えばＲＯＭ６０２に格納されてＣＰＵ６０１によって処理されるか、あるいはハードディスクに格納されＨＤＤ６０４を介してＣＰＵ６０１に供給されて実行される。

【０４９２】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０４９３】なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフト

ウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０４９４】例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read OnlyMemory)に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Maqneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０４９５】なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０４９６】なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０４９７】

【発明の効果】以上、説明したように、本発明のバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、情報処理装置において、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータを生成するとともに、バックアップ鍵を外部エンティテイであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成としたので、第三者にバックアップデータを格納したメディアが渡ったとしても復号される恐れがなく、ユーザデバイスにおけるバックアップデータ管理の負担が軽減され、データの高度なセキュリティの下での管理が容易となる。

【０４９８】また、本発明のバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、サポートセンタにおけるバックアップデータのリストア処理は、メモリ領域確保用属性証明書に従って情報処理装置のメモリ内に区分領域を設定し、設定した区分領域にバックアップデータを格納する処理として実行する構成であるので、属性証明書の検証により、正当性の立証された属性証明書に基づいて、メモリ領域が設定され、データのリストアが実行されるので、不正なデータリストアを防止することが可能となる。

【図面の簡単な説明】

【図１】本発明のコンテンツ利用管理システム構成の概要を説明する図である。

【図２】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図３】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図４】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図５】本発明のコンテンツ利用管理システムにおいて適用可能な権限情報証明書としての属性証明書のフォーマットを示す図である。

【図６】ユーザデバイスにおけるセキュリティチップの構成を示す構成図である。

【図７】ユーザデバイス内での処理対象となる主なデータを示す図である。

【図８】認証情報（パスワード）の初期登録処理シーケンスを示す図である。

【図９】認証情報（パスワード）の変更処理シーケンスを示す図である。

【図１０】認証情報（パスワード）の変更処理シーケンスを示す図である。

【図１１】認証情報（パスワード）とマスタパスワードとの対応について説明する図である。

【図１２】マスタパスワードの配布処理について説明する図である。

【図１３】マスタパスワードの再発行処理シーケンスを示す図である。

【図１４】マスタパスワードの算出処理を示すフロー図である。

【図１５】属性証明書（ＡＣ）発行、コンテンツ受信処理シーケンスを示す図である。

【図１６】相互認証処理の例であるＴＬＳ１．０ハンドシェイクプロトコルのシーケンスを示す図である。

【図１７】データ改竄検証に適用するＭＡＣの生成処理を説明する図である。

【図１８】属性証明書（ＡＣ）の発行処理シーケンスを示す図である。

【図１９】署名生成処理の例であるＥＣＤＳＡ署名生成手順を説明するフロー図である。

【図２０】署名検証処理の例であるＥＣＤＳＡ署名検証

手順を説明するフロー図である。
【図２１】公開鍵証明書（ＰＫＣ）と属性証明書（ＡＣ）との関連付けについて説明する図である。
【図２２】公開鍵証明書（ＰＫＣ）の検証処理フローを示す図である。
【図２３】属性証明書（ＡＣ）の検証処理フロー（例１）を示す図である。
【図２４】属性証明書（ＡＣ）の検証処理フロー（例２）を示す図である。
【図２５】属性証明書（ＡＣ）を利用したコンテンツ利用処理（オフライン）を説明するシーケンス図である。
【図２６】属性証明書（ＡＣ）を利用したコンテンツ利用処理（オンライン）を説明するシーケンス図である。
【図２７】グローバル共通鍵によるコンテンツ鍵の暗号化データを格納した属性証明書（ＡＣ）を利用したコンテンツ利用処理（オフライン）を説明する図である。
【図２８】グローバル共通鍵の更新処理を説明するシーケンス図である。
【図２９】グローバル共通鍵の更新処理を説明するシーケンス図である。
【図３０】デコーダを用いた復号化処理について説明する図である。
【図３１】デコーダを用いた復号化処理シーケンスについて説明する図である。
【図３２】デコーダを用いた復号化処理フローについて説明する図である。
【図３３】ユーザデバイス側における属性証明書（ＡＣ）の適用処理を説明するフロー図である。
【図３４】属性証明書（ＡＣ）を利用したオンライン期間制限コンテンツの利用処理を説明するシーケンス図である。
【図３５】属性証明書（ＡＣ）を利用したオンライン回数制限コンテンツの利用処理を説明するシーケンス図である。
【図３６】属性証明書（ＡＣ）を利用したオフライン買い切りコンテンツの利用処理を説明するシーケンス図である。
【図３７】オフライン回数制限コンテンツに対応する利用回数管理データのインポート処理を説明する図である。
【図３８】オフライン回数制限コンテンツに対応する利用回数管理データのデータ構成例を示す図である。
【図３９】オフライン回数制限コンテンツに対応する利用回数管理データのインポート処理を説明するフロー図である。
【図４０】オフライン回数制限コンテンツに対応するハッシュ値管理型の利用回数管理データのインポート処理を説明する図である。
【図４１】オフライン回数制限コンテンツに対応するハッシュ値管理型の利用回数管理データのインポート処理を説明するフロー図である。
【図４２】オフライン回数制限コンテンツの属性証明書を適用したコンテンツ利用処理を説明する図である。
【図４３】オフライン回数制限コンテンツに対応する回数管理データの更新処理を説明する図である。
【図４４】オフライン回数制限コンテンツに対応するハッシュ値管理型の回数管理データの更新処理を説明する図である。
【図４５】オンライン期間制限属性証明書をベースとして適用したアップグレード処理を説明する図である。
【図４６】オンライン回数制限属性証明書をベースとして適用したアップグレード処理を説明する図である。
【図４７】オフライン回数制限属性証明書をベースとして適用したアップグレード処理を説明する図である。
【図４８】アルバム購入型のアップグレード処理を説明する図である。
【図４９】サポートセンタによるデータリストア処理の概要を説明する図である。
【図５０】サポートセンタによるデータリストア処理の処理シーケンス概要を説明する図である。
【図５１】ユーザデバイス側で実行するデータバックアップ処理シーケンスを説明する図である。
【図５２】サポートセンタによるバックアップデータ読み出し処理の概要を説明する図である。
【図５３】サポートセンタによるデータリストア処理シーケンスを説明する図である。
【図５４】ユーザデバイスの構成例を示す図である。
【図５５】サービスプロバイダ、サポートセンタ、コンテンツクリエータ等の各エンティティの構成例を示す図である。

【符号の説明】

１０１　ユーザデバイス
１０２　サービスプロバイダ
１０３　コンテンツクリエータ
１０４　ユーザデバイス製造者
１０５　サポートセンタ
１０６　認証局
１１０　属性証明書
２００　ユーザデバイス
２０１　ＣＰＵ（Central processing Unit）
２０２　インタフェース
２０３　ＲＯＭ（Read-Only-Memory）
２０４　ＲＡＭ（Random Access Memory）
２０５　暗号処理部
２０６　メモリ部
２１０　セキュリティチップ
２２１　ユーザデバイス側制御部
２２２　外部メモリ部
２８０　デコーダ
３０１　システムホルダ

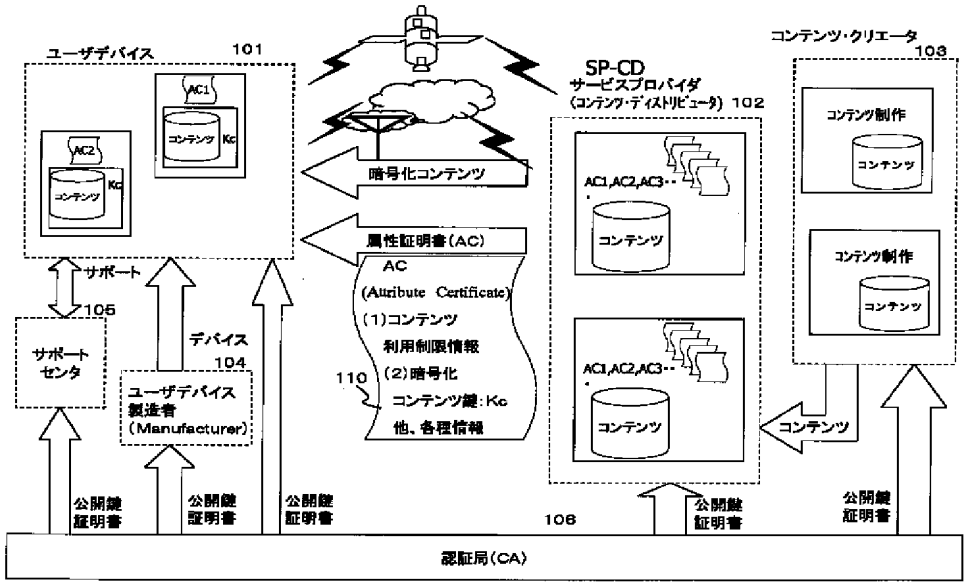
105

３０２　サービスプロバイダ
３０３　コンテンツクリエータ
３０４　ユーザデバイス
４１０　ユーザデバイス
４１１　セキュリティチップ
４２１　記憶手段
４２２　ストレージメディア
４３０　ユーザデバイス
４５０　サポートセンタ
４７０　ユーザデバイス
４７１　ストレージメディア
４７２　ユーザデバイス
４７５　サポートセンタ
５０１　ＣＰＵ（Central processing Unit）
５０２　ＲＯＭ（Read-Only-Memory）
５０３　ＲＡＭ（Random Access Memory）
５０４　ＨＤＤ

106

＊５０５　入力部
５０６　出力部
５０７　通信部
５０８　ドライブ
５０９　リムーバブル記録媒体
５１０　バス
５１１　入出力インタフェース
５１２　セキュリティチップ
６０１　ＣＰＵ(Central processing Unit)
６０２　ＲＯＭ（Read-Only-Memory）
６０３　ＲＡＭ（Random Access Memory）
６０４　ＨＤＤ
６０５　暗号処理手段
６０６　ドライブ
６０７　リムーバブル記録媒体
６０８，６０９　通信部
＊　６１０　バス

【図１】



【図２】

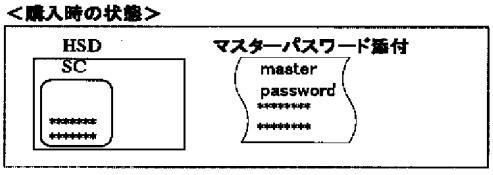
Version		
V-1	version	証明書のフォーマットのバージョン
	serialNumber	証明書発行者によって割り当てられる証明書番号
	signature	証明書の署名アルゴリズム
	Issuer	証明書発行者名(Distinguished Name形式)
	validity notBefore notAfter	証明書の有効期限 開始日時 終了日時
	subject	証明書所有者名
	subjectPublicKeyInfo algorithm subjectPublickey	証明書所有者の公開鍵情報 鍵のアルゴリズム 鍵

【図３】

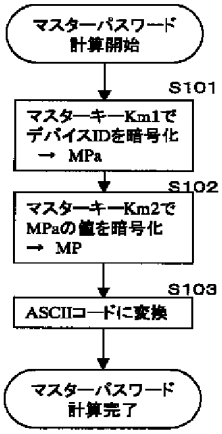
V-3	authorityKeyIdentifier keyIdentifier authorityCertIssuer authorityCertSerialNumber	署名検証に用いる証明書発行者の鍵識別子 鍵識別子 機関証明書発行者名(General Name形式) 機関証明書シリアルナンバ
	subjectKeyIdentifier keyIdentifier	複数の鍵の中から目的の鍵を明確に識別
	key usage (0)digitalSignature (1)nonRepudiation (2)keyEncipherment (3)dataEncipherment (4)keyAgreement (5)keyCertSign (6)cRLSign	鍵の使用目的を指定 (0)デジタル署名用 (1)否認防止用 (2)鍵の暗号化用 (3)メッセージの暗号化用 (4)共通鍵配送用 (5)認証の署名確認用 (6)失効リストの署名確認用
	privateKeyUsagePeriod notBefore notAfter	証明書中の公開鍵に対応する秘密鍵の有効期限
	certificatePolicies policyIdentifier policyQualifiers	証明書発行者が承認した証明書ポリシー ポリシーID(ISO/IEC9834-1準拠) 認証基準
	policyMappings IssuerDomainPolicy subjectDomainPolicy	認証パス中のポリシーの関係を制限 （CA証明書にのみ必要）

【図１２】

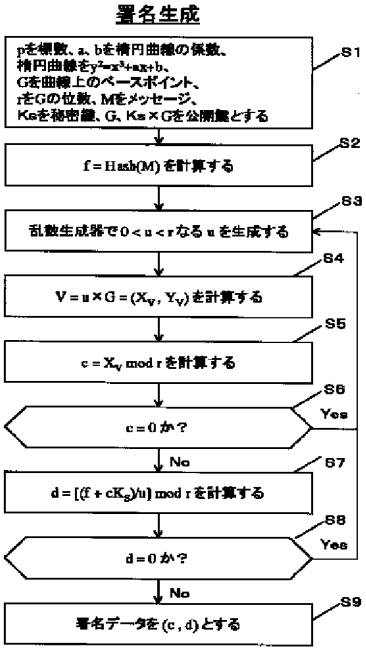
<＜購入時の状態＞



【図１４】



【図１９】

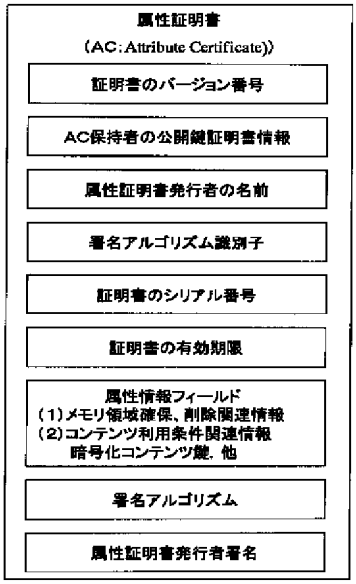


署名生成(IEEE P1363/D13)

【図４】

V-3	subjectAltName	証明書所有者の別名（GN形式）
	issuerAltName	証明書発行者の別名（GN形式）
	subjectDirectoryAttributes	証明書所有者のために必要とされるディレクトリの属性
	basicConstraints cA pathLenConstraint	証明対象の公開鍵が認証局の署名用か、証明書所有者のものかを区別
	nameConstraints permittedSubtrees base minimum maximum ExcludedSubtrees	発行者が発行する証明書の名前を制限
	policyConstraints requireExplicitPolicy inhibitPolicyMapping	認証パス中のポリシーの関係を制限
	cRLDistributionPoints	証明書所有者が証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照点を記述
	signatureAlgorithm	証明書への署名付けに用いるアルゴリズム
	signatureValue	証明書発行者の秘密鍵による署名

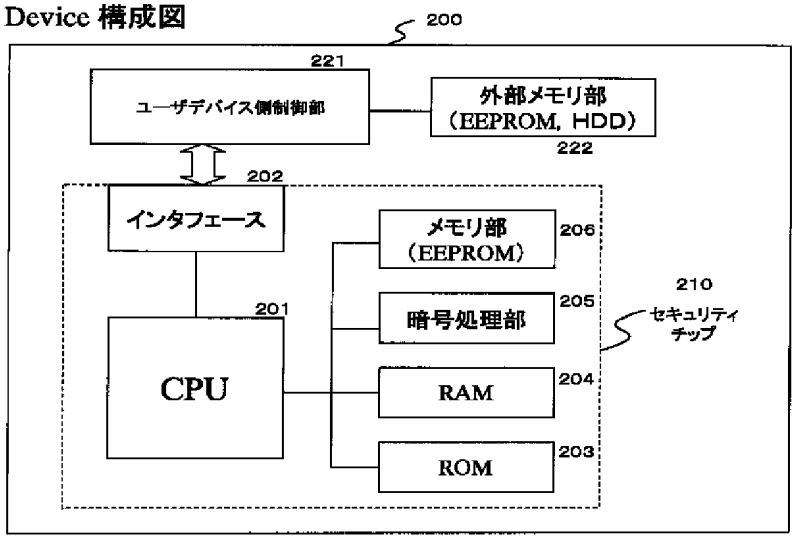
【図５】



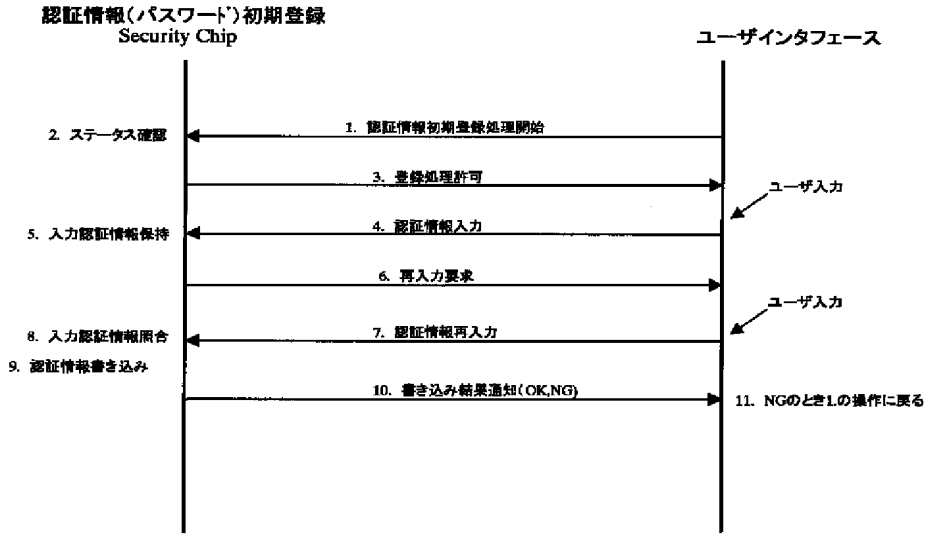
【図７】

データ種別	データ内容
公開鍵証明書	・ルート認証局公開鍵証明書 ・サービスプロバイダ公開鍵証明書 ・サポートセンタ公開鍵証明書
属性証明書	・アプリケーション(コンテンツ)利用管理用 属性証明書 ・SP用メモリ領域管理用属性証明書
鍵データ	・公開鍵、秘密鍵ペア ・ストレージ鍵 (デバイス対応ストレージ鍵:グローバル共通鍵) (サービスプロバイダ対応ストレージ鍵) ・乱数生成用鍵、・相互認証用鍵
識別情報	・デバイスID ・サービスプロバイダID ・ユーザID ・アプリケーションID
その他	・認証情報 ・乱数シード(Seed) ・コンテンツ利用回数情報

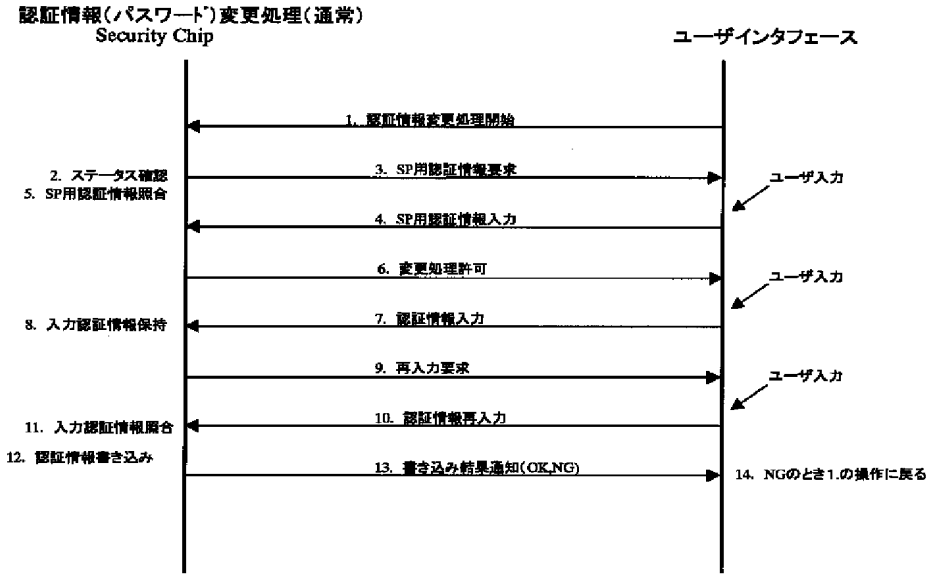
【図６】


Device 構成図
200
221
ユーザデバイス側制御部
外部メモリ部
（EEPROM, HDD）
222
202
インタフェース
メモリ部
（EEPROM）
206
210
セキュリティ
チップ
201
暗号処理部
205
CPU
RAM
204
ROM
203

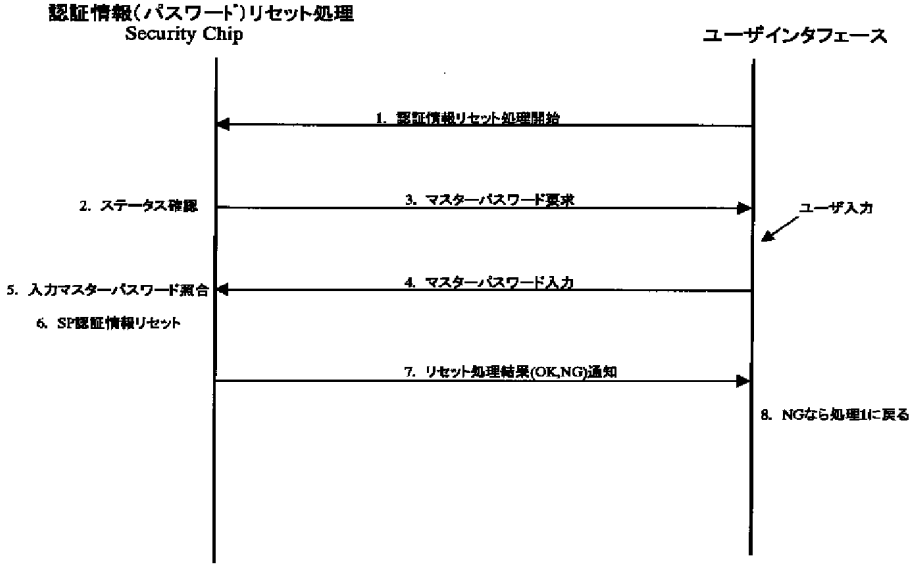
【図８】


認証情報（パスワード）初期登録
Security Chip
ユーザインタフェース
2. ステータス確認
1. 認証情報初期登録処理開始
3. 登録処理許可
ユーザ入力
5. 入力認証情報保持
4. 認証情報入力
6. 再入力要求
ユーザ入力
8. 入力認証情報照合
7. 認証情報再入力
9. 認証情報書き込み
10. 書き込み結果通知（OK,NG）
11. NGのとき1.の操作に戻る

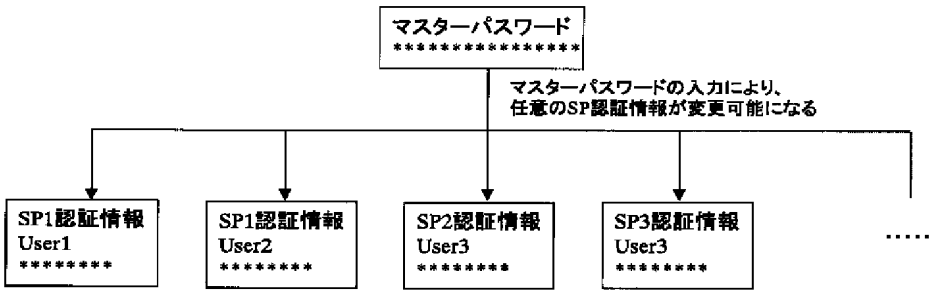
【図９】


認証情報(パスワード)変更処理(通常)
Security Chip
ユーザインタフェース
1. 認証情報変更処理開始
2. ステータス確認
3. SP用認証情報要求
ユーザ入力
5. SP用認証情報照合
4. SP用認証情報入力
6. 変更処理許可
ユーザ入力
8. 入力認証情報保持
7. 認証情報入力
9. 再入力要求
ユーザ入力
11. 入力認証情報照合
10. 認証情報再入力
12. 認証情報書き込み
13. 書き込み結果通知(OK,NG)
14. NGのとき1.の操作に戻る

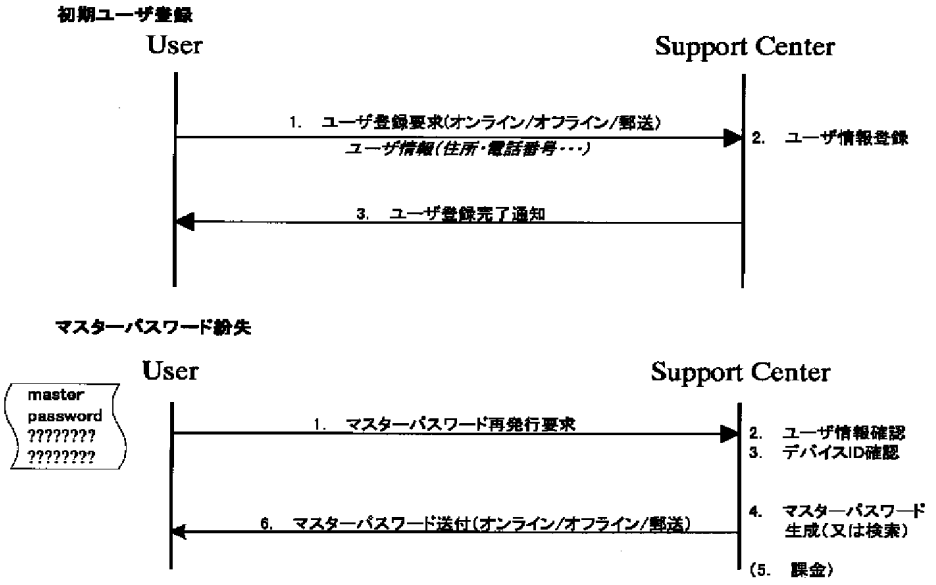
【図１０】


認証情報(パスワード)リセット処理
Security Chip
ユーザインタフェース
1. 認証情報リセット処理開始
2. ステータス確認
3. マスターパスワード要求
ユーザ入力
5. 入力マスターパスワード照合
4. マスターパスワード入力
6. SP認証情報リセット
7. リセット処理結果(OK,NG)通知
8. NGなら処理1に戻る

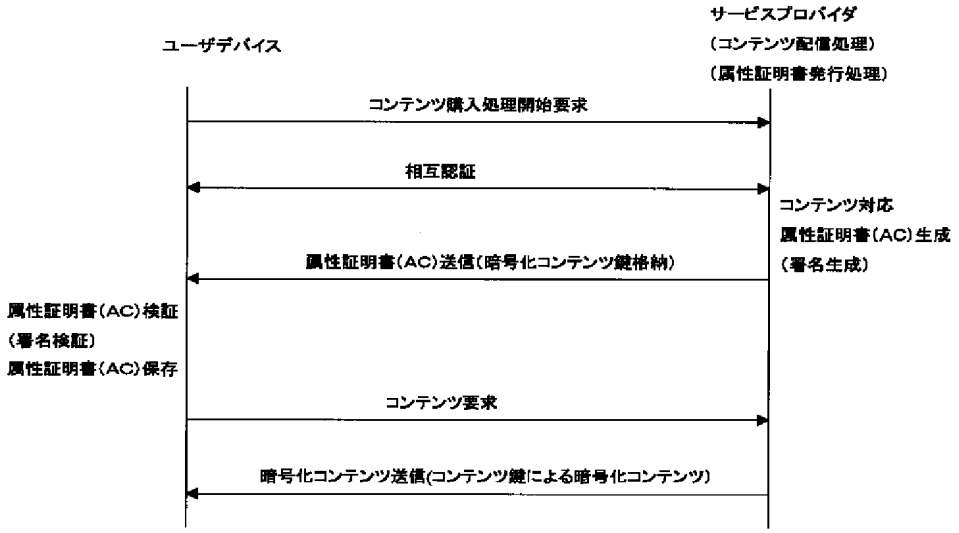
【図１１】


マスターパスワード
****
マスターパスワードの入力により、
任意のSP認証情報が変更可能になる
SP1認証情報
User1
****
SP1認証情報
User2
****
SP2認証情報
User3
****
SP3認証情報
User3
****
.....

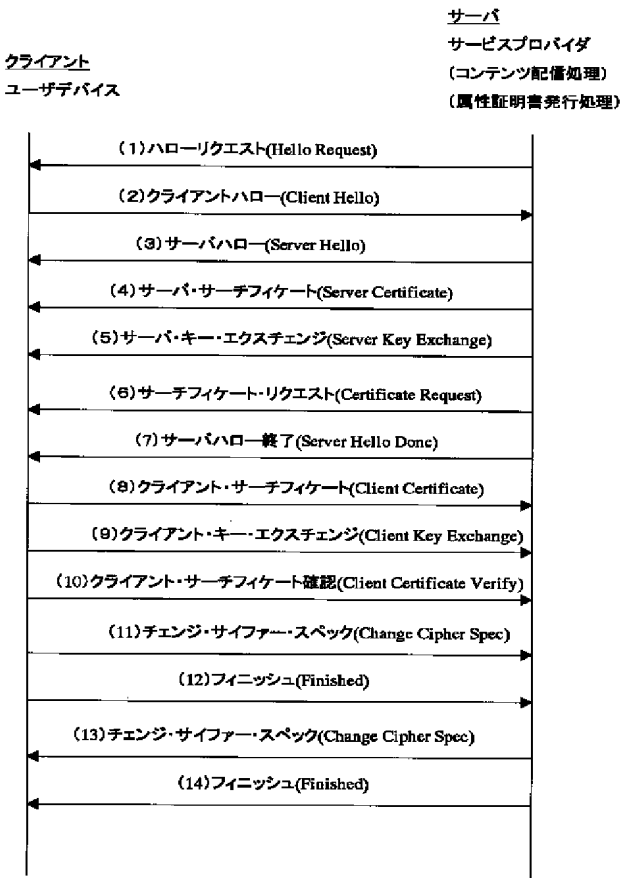
【図１３】


初期ユーザ登録
User
Support Center
1. ユーザ登録要求(オンライン/オフライン/郵送)
ユーザ情報(住所・電話番号・・・)
2. ユーザ情報登録
3. ユーザ登録完了通知
マスターパスワード紛失
User
Support Center
master
password
????????
????????
1. マスターパスワード再発行要求
2. ユーザ情報確認
3. デバイスID確認
4. マスターパスワード
生成(又は検索)
6. マスターパスワード送付(オンライン/オフライン/郵送)
(5. 課金)

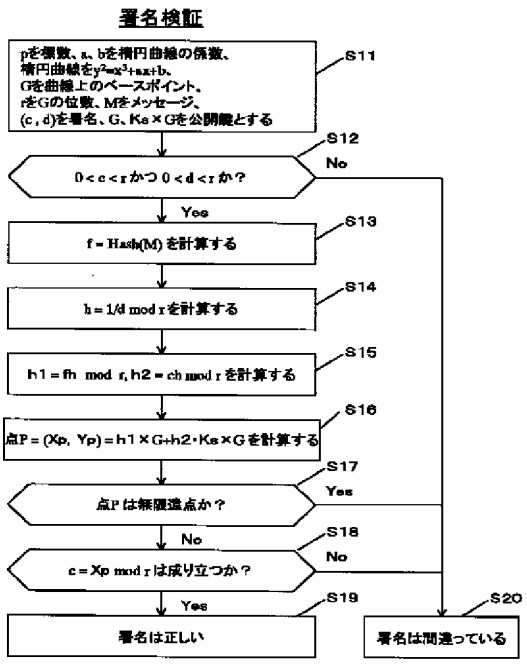
【図１５】



【図１６】

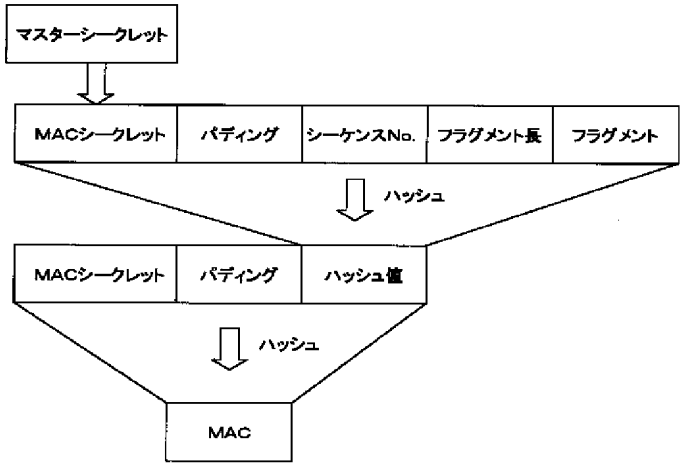


【図２０】

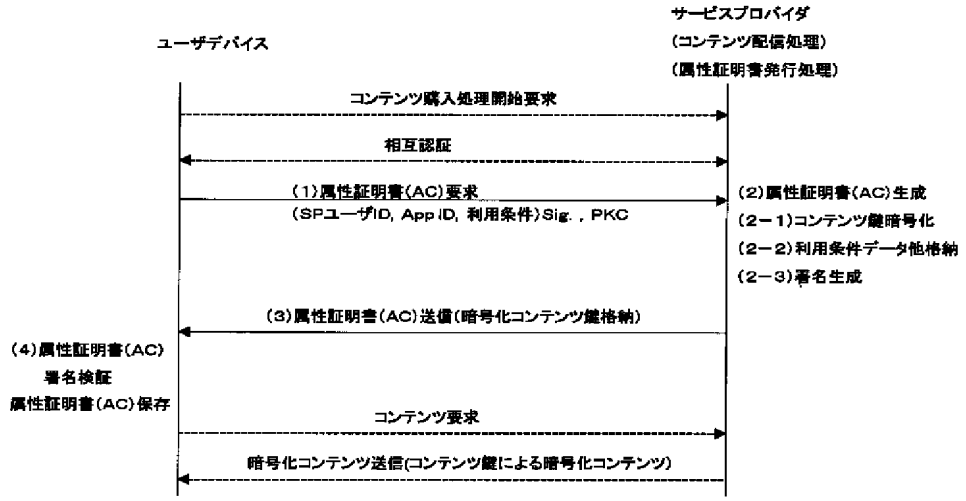


署名検証（IEEE P1363/D13）

【図１７】

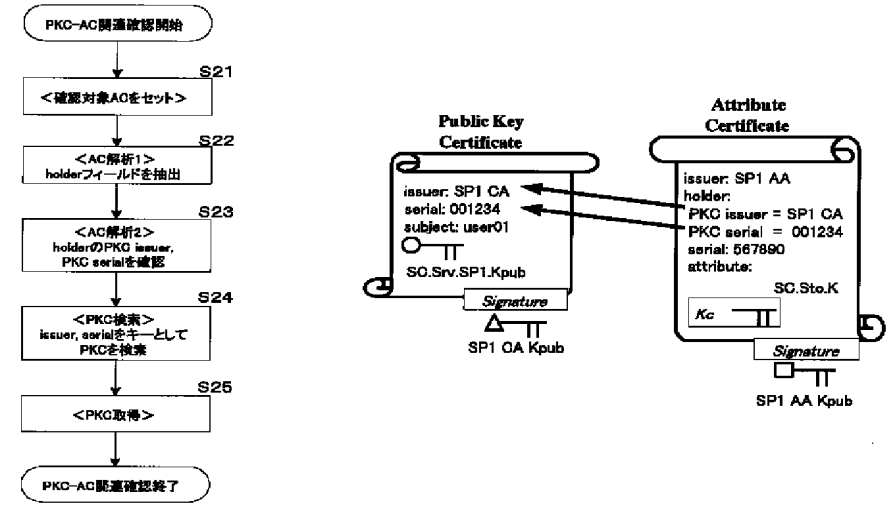

マスターシークレット
MACシークレット
パディング
シーケンスNo.
フラグメント長
フラグメント
ハッシュ
MACシークレット
パディング
ハッシュ値
ハッシュ
MAC

【図１８】

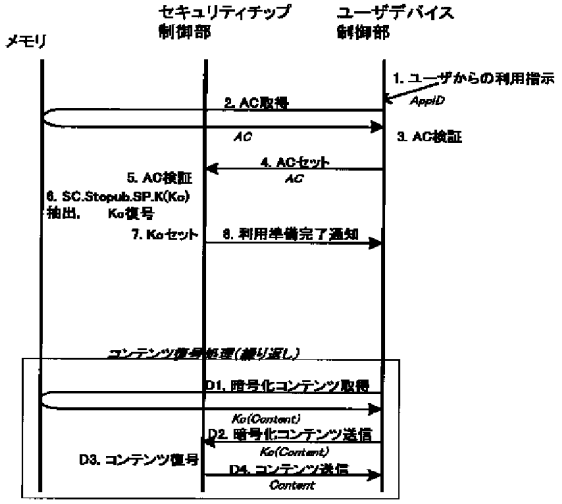

ユーザデバイス
サービスプロバイダ
(コンテンツ配信処理)
(属性証明書発行処理)
コンテンツ購入処理開始要求
相互認証
(1)属性証明書(AC)要求
(SPユーザID, App ID, 利用条件)Sig. , PKC
(2)属性証明書(AC)生成
(2－1)コンテンツ鍵暗号化
(2－2)利用条件データ他格納
(2－3)署名生成
(3)属性証明書(AC)送信(暗号化コンテンツ鍵格納)
(4)属性証明書(AC)
署名検証
属性証明書(AC)保存
コンテンツ要求
暗号化コンテンツ送信(コンテンツ鍵による暗号化コンテンツ)

【図２１】

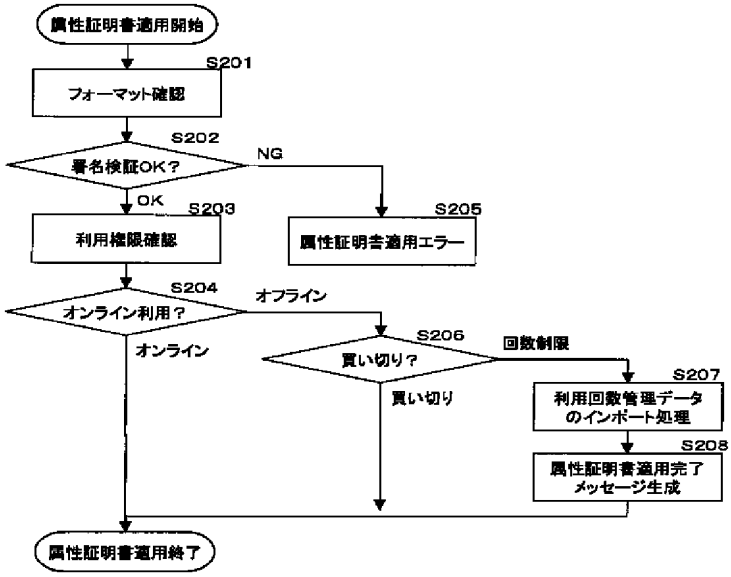
PKCとACの関連づけ



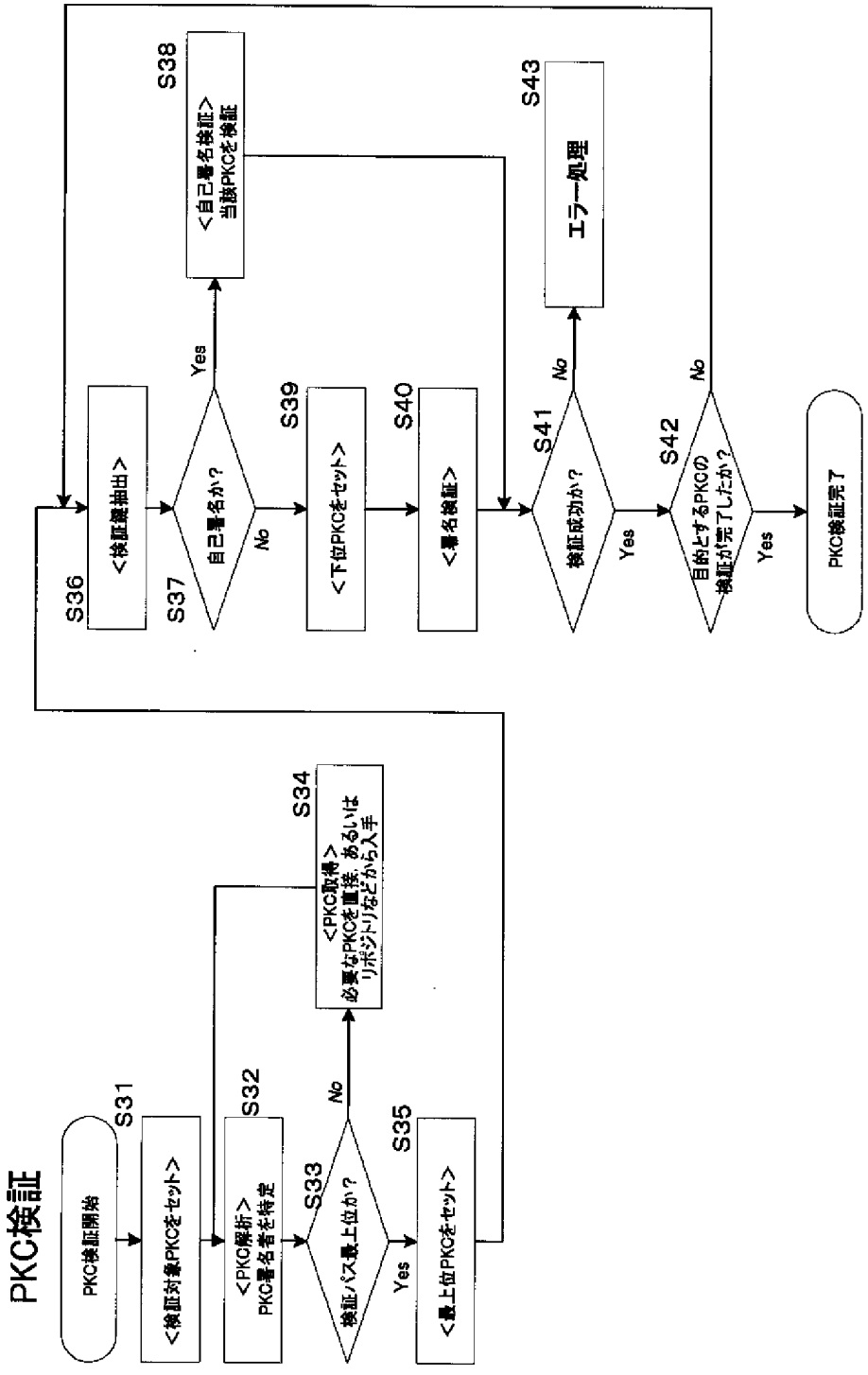
【図２５】



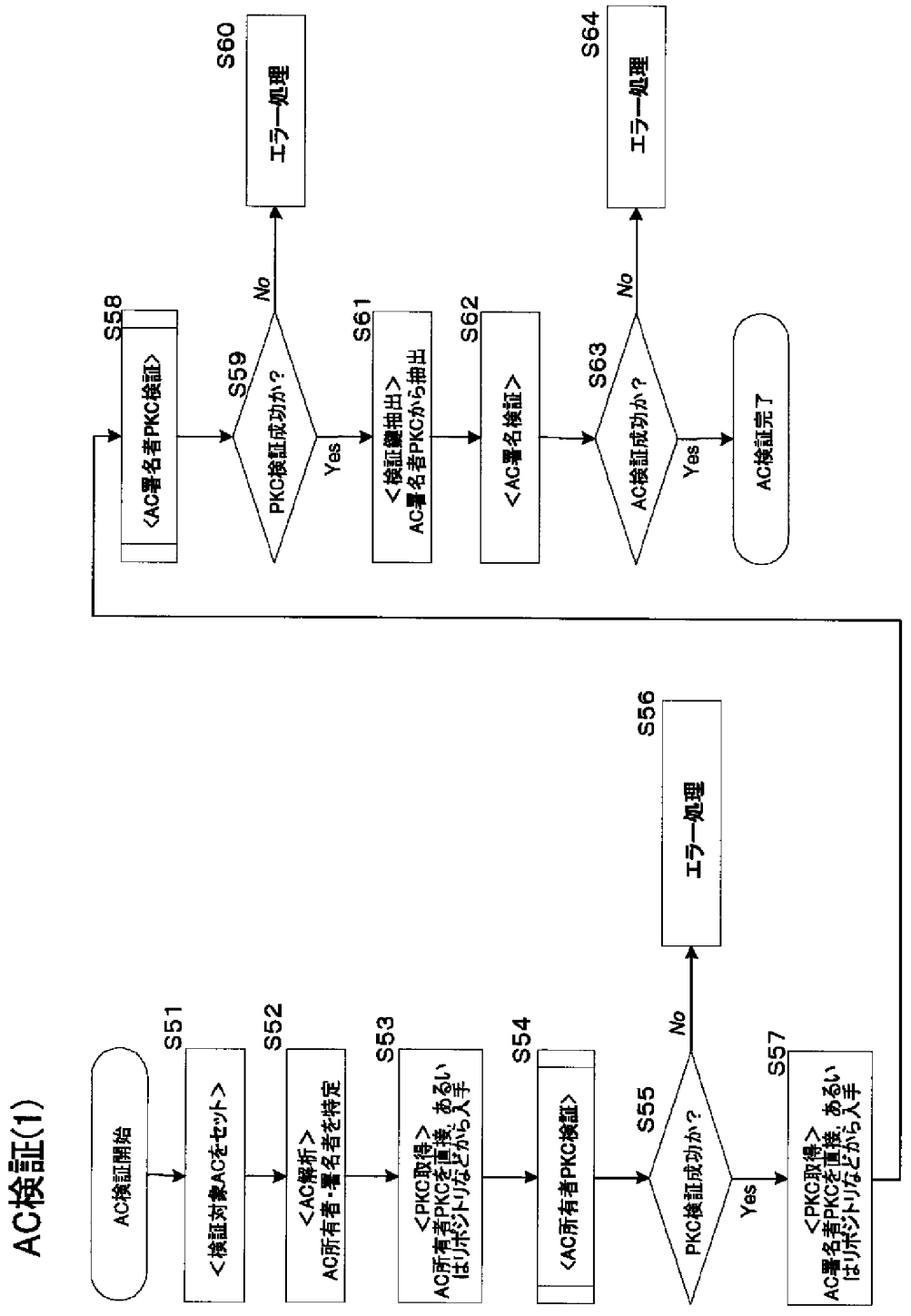
【図３３】



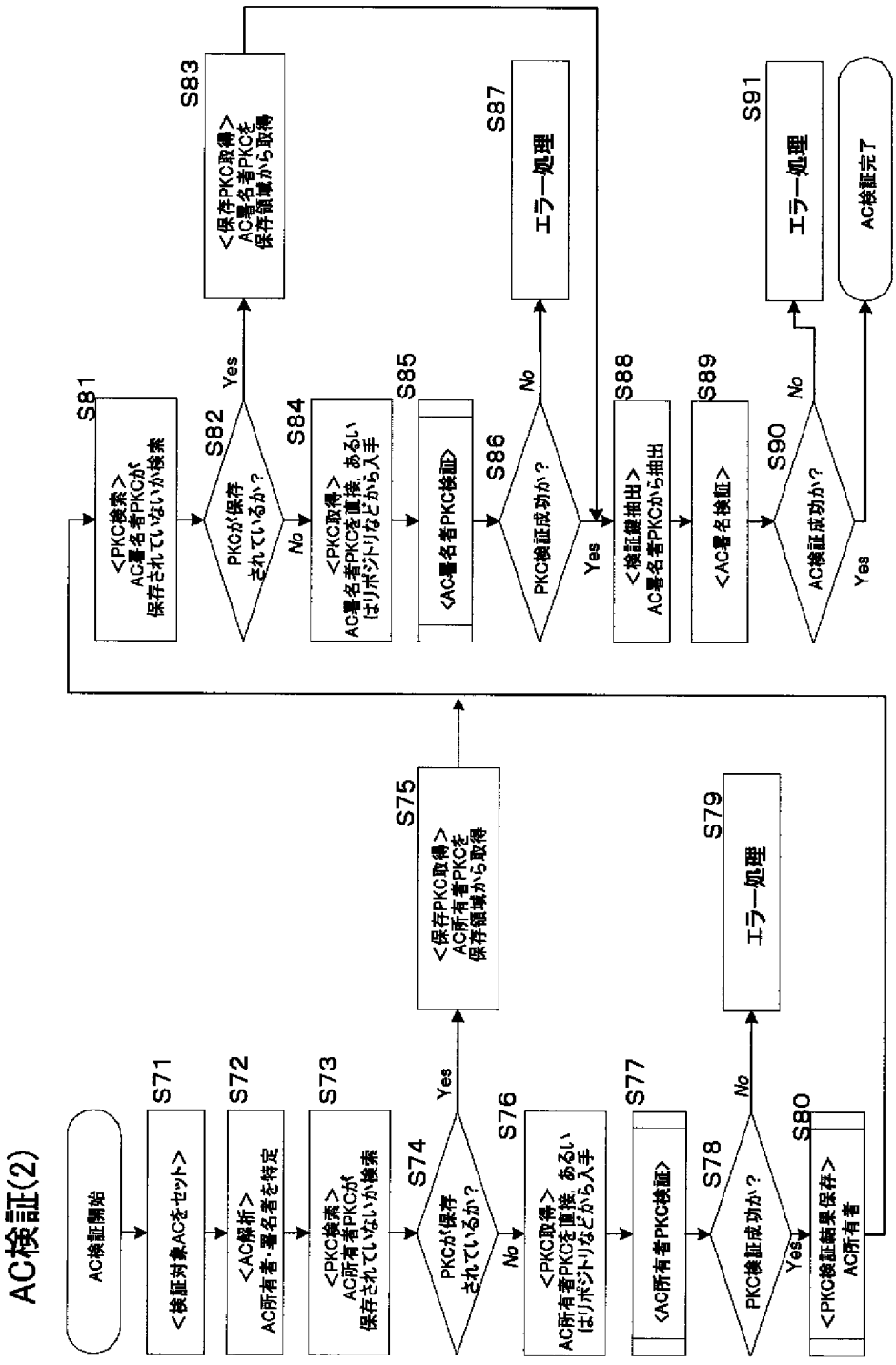
【図２２】


PKC検証
PKC検証開始
S31
<検証対象PKCをセット>
S32
<PKC解析>
PKC署名者を特定
S33
検証パス最上位か？
No
S34
<PKC取得>
必要なPKCを直接 あるいは
リポジトリなどから入手
Yes
S35
<最上位PKCをセット>
S36
<検証鍵抽出>
S37
自己署名か？
Yes
S38
<自己署名検証>
当該PKCを検証
No
S39
<下位PKCをセット>
S40
<署名検証>
S41
検証成功か？
No
S43
エラー処理
Yes
S42
目的とするPKCの
検証が完了したか？
No
Yes
PKC検証完了

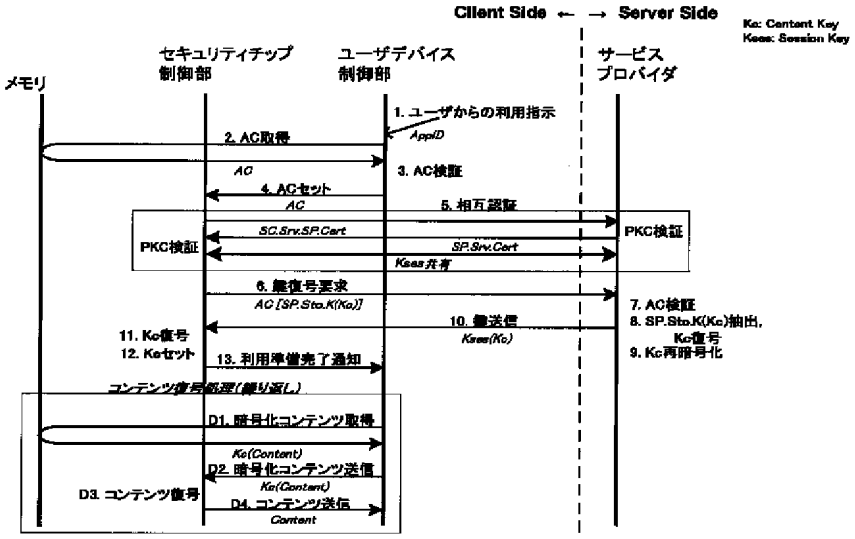
【図２３】


AC検証(1)
AC検証開始
S51
<検証対象ACをセット>
S52
<AC解析>
AC所有者・署名者を特定
S53
<PKC取得>
AC所有者PKCを直接、あるいはリポジトリなどから入手
S54
<AC所有者PKC検証>
S55
PKC検証成功か？
No
S56
エラー処理
Yes
S57
<PKC取得>
AC署名者PKCを直接、あるいはリポジトリなどから入手
S58
<AC署名者PKC検証>
S59
PKC検証成功か？
No
S60
エラー処理
Yes
S61
<検証鍵抽出>
AC署名者PKCから抽出
S62
<AC署名検証>
S63
AC検証成功か？
No
S64
エラー処理
Yes
AC検証完了

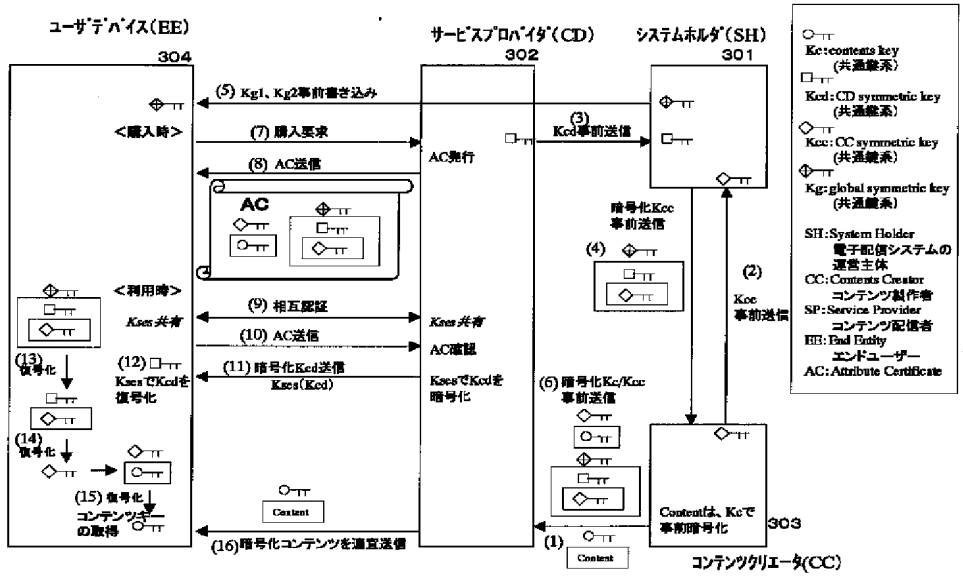
【図２４】


AC検証(2)
AC検証開始
S71
<検証対象ACをセット>
S72
<AC解析>
AC所有者・署名者を特定
S73
<PKC検索>
AC所有者PKCが
保存されていないか検索
S74
PKCが保存
されているか？
Yes
No
S75
<保存PKC取得>
AC所有者PKCを
保存領域から取得
S76
<PKC取得>
AC所有者PKCを直接、あるい
はリポジトリなどから入手
S77
<AC所有者PKC検証>
S78
PKC検証成功か？
No
Yes
S79
エラー処理
S80
<PKC検証結果保存>
AC所有者
S81
<PKC検索>
AC署名者PKCが
保存されていないか検索
S82
PKCが保存
されているか？
Yes
No
S83
<保存PKC取得>
AC署名者PKCを
保存領域から取得
S84
<PKC取得>
AC署名者PKCを直接、あるい
はリポジトリなどから入手
S85
<AC署名者PKC検証>
S86
PKC検証成功か？
No
Yes
S87
エラー処理
S88
<検証鍵抽出>
AC署名者PKCから抽出
S89
<AC署名検証>
S90
AC検証成功か？
No
Yes
S91
エラー処理
AC検証完了

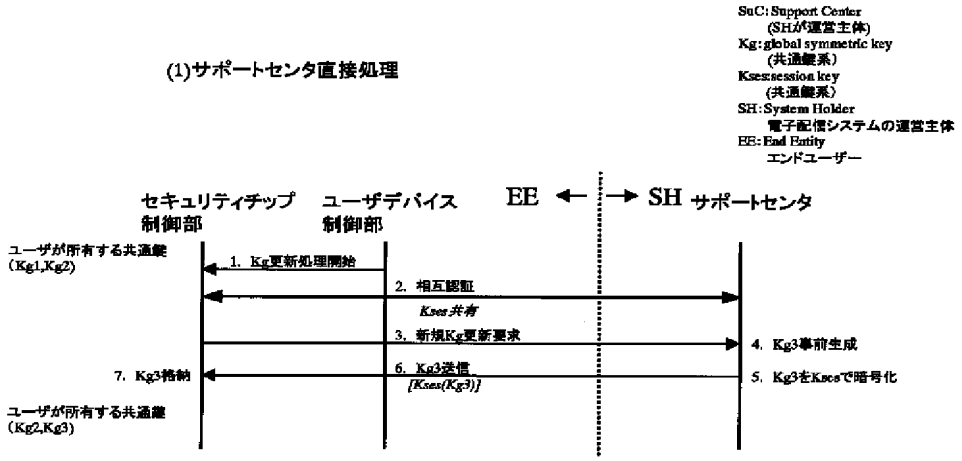
【図２６】


Client Side ← → Server Side
Kc: Content Key
Kses: Session Key
メモリ
セキュリティチップ 制御部
ユーザデバイス 制御部
サービス プロバイダ
1. ユーザからの利用指示
AppID
2. AC取得
AC
3. AC検証
4. ACセット
AC
5. 相互認証
SC.Srv.SP.Cert
SP.Srv.Cert
Kses共有
PKC検証
PKC検証
6. 鍵復号要求
AC [SP.Sto.K(Kc)]
7. AC検証
8. SP.Sto.K(Kc)抽出, Kc復号
9. Kc再暗号化
10. 鍵送信
Kses(Kc)
11. Kc復号
12. Kcセット
13. 利用準備完了通知
コンテンツ復号処理(繰り返し)
D1. 暗号化コンテンツ取得
Kc(Content)
D2. 暗号化コンテンツ送信
Kc(Content)
D3. コンテンツ復号
D4. コンテンツ送信
Content

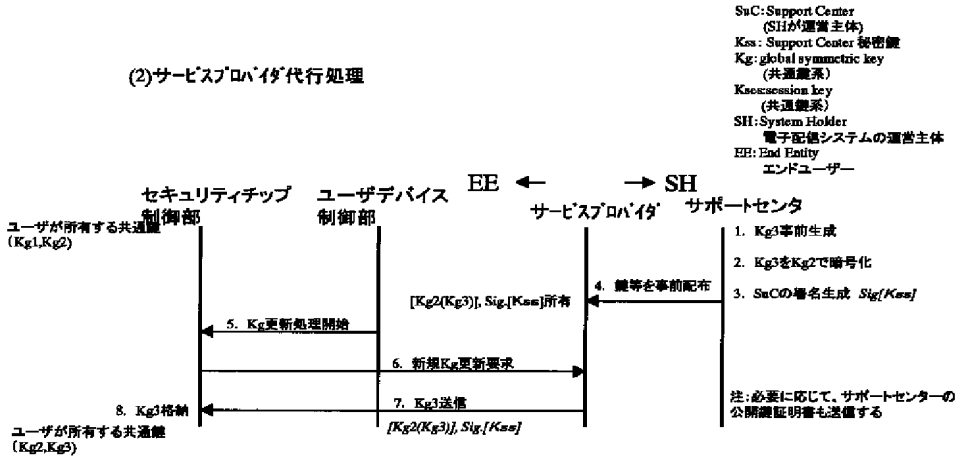
【図２７】


ユーザデバイス(EE)
304
サービスプロバイダ(CD)
302
システムホルダ(SH)
301
<購入時>
(5) Kg1、Kg2事前書き込み
(7) 購入要求
(8) AC送信
AC発行
(3) Kcd事前送信
AC
暗号化Kcc 事前送信
(4)
(2) Kcc 事前送信
<利用時>
Kses共有
(9) 相互認証
Kses共有
(10) AC送信
AC確認
(13) 復号化
(12) KsesでKcdを復号化
(11) 暗号化Kcd送信
Kses(Kcd)
KsesでKcdを暗号化
(6) 暗号化Kc/Kcc 事前送信
(14) 復号化
(15) 復号化 コンテンツキーの取得
Content
(16)暗号化コンテンツを直接送信
Contentは、Kcで事前暗号化
303
(1)
Content
コンテンツクリエータ(CC)
Kc:contents key (共通鍵系)
Kcd:CD symmetric key (共通鍵系)
Kcc:CC symmetric key (共通鍵系)
Kg:global symmetric key (共通鍵系)
SH:System Holder 電子配信システムの運営主体
CC:Contents Creator コンテンツ製作者
SP:Service Provider コンテンツ配信者
EE:End Entity エンドユーザー
AC:Attribute Certificate

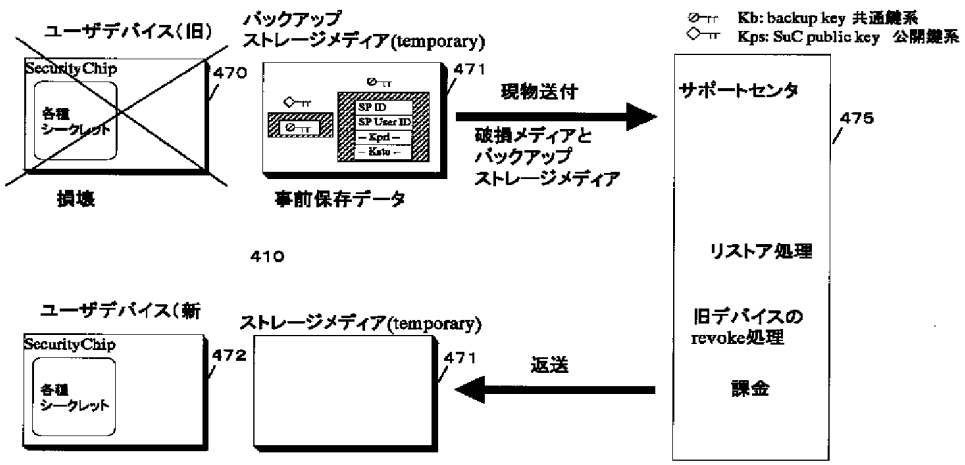
【図２８】


SuC: Support Center
(SHが運営主体)
Kg: global symmetric key
(共通鍵系)
Kses:session key
(共通鍵系)
SH: System Holder
電子配信システムの運営主体
EE: End Entity
エンドユーザー
(1)サポートセンタ直接処理
セキュリティチップ制御部
ユーザデバイス制御部
EE
SH サポートセンタ
ユーザが所有する共通鍵
(Kg1,Kg2)
1. Kg更新処理開始
2. 相互認証
Kses共有
3. 新規Kg更新要求
4. Kg3事前生成
5. Kg3をKsesで暗号化
6. Kg3送信
[Kses(Kg3)]
7. Kg3格納
ユーザが所有する共通鍵
(Kg2,Kg3)

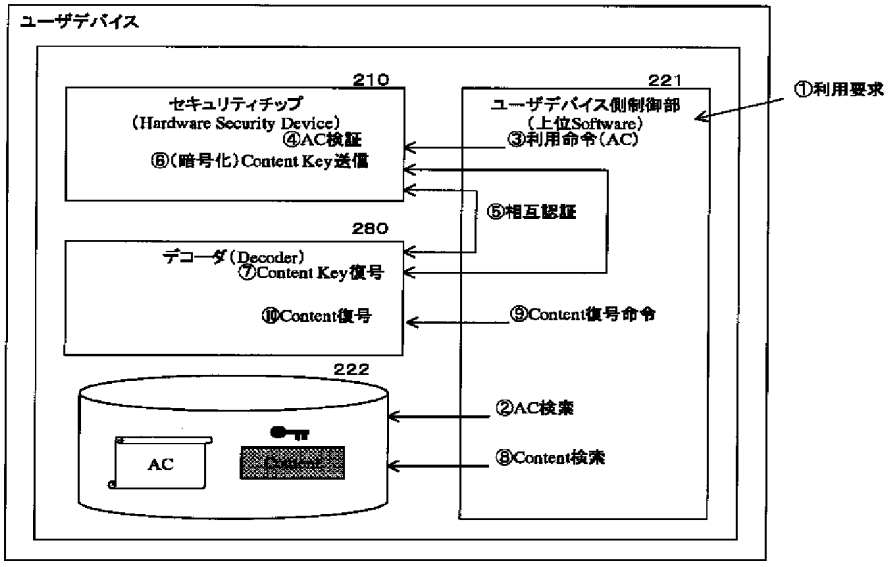
【図２９】


SuC: Support Center
(SHが運営主体)
Kss: Support Center 秘密鍵
Kg: global symmetric key
(共通鍵系)
Kses:session key
(共通鍵系)
SH: System Holder
電子配信システムの運営主体
EE: End Entity
エンドユーザー
(2)サービスプロバイダ代行処理
セキュリティチップ制御部
ユーザデバイス制御部
EE
SH
サービスプロバイダ
サポートセンタ
ユーザが所有する共通鍵
(Kg1,Kg2)
1. Kg3事前生成
2. Kg3をKg2で暗号化
3. SuCの署名生成 Sig[Kss]
4. 鍵等を事前配布
[Kg2(Kg3)], Sig.[Kss]所有
5. Kg更新処理開始
6. 新規Kg更新要求
7. Kg3送信
[Kg2(Kg3)], Sig.[Kss]
8. Kg3格納
ユーザが所有する共通鍵
(Kg2,Kg3)
注:必要に応じて、サポートセンターの公開鍵証明書も送信する

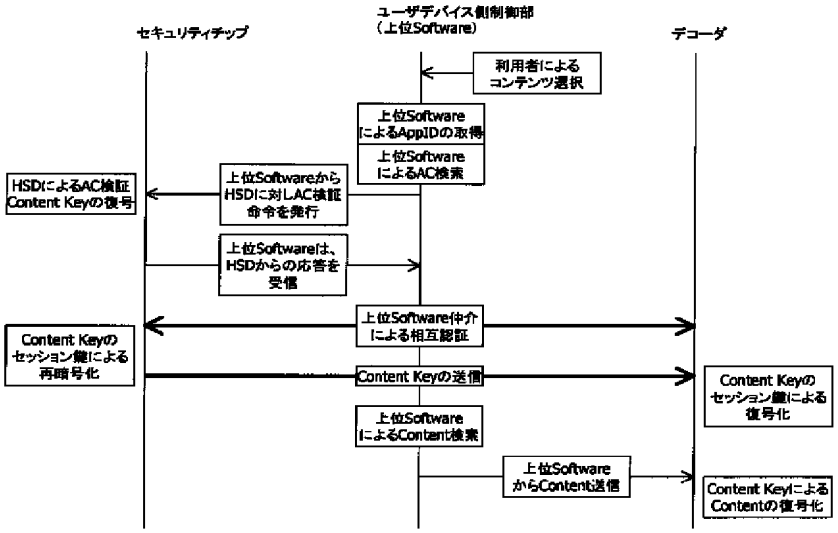
【図５０】


Kb: backup key 共通鍵系
Kps: SuC public key 公開鍵系
ユーザデバイス(旧)
バックアップストレージメディア(temporary)
SecurityChip
各種シークレット
470
SP ID
SP User ID
Kpd
Kstu
471
現物送付
破損メディアとバックアップストレージメディア
サポートセンタ
475
損壊
事前保存データ
410
リストア処理
旧デバイスのrevoke処理
課金
ユーザデバイス(新
ストレージメディア(temporary)
SecurityChip
各種シークレット
472
471
返送

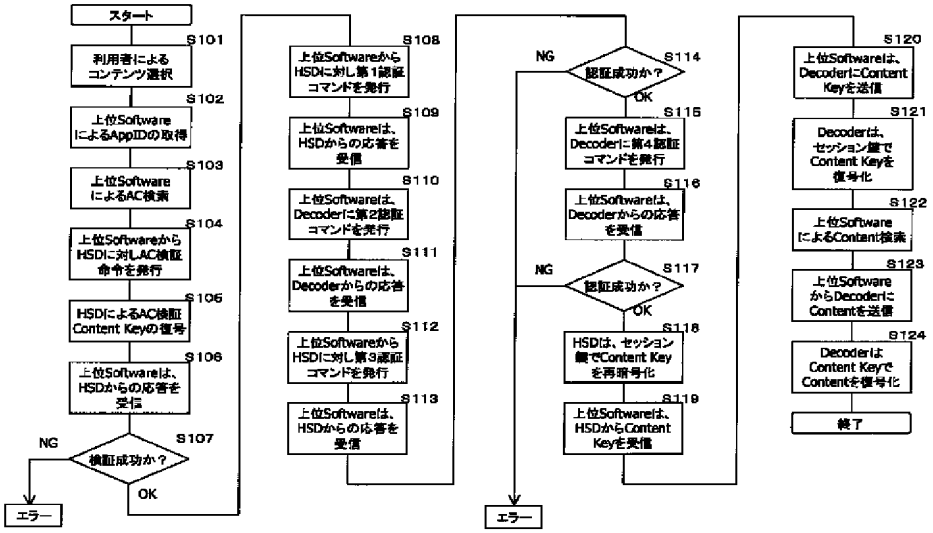
【図３０】


ユーザデバイス
210
セキュリティチップ
(Hardware Security Device)
④AC検証
⑥(暗号化)Content Key送信
221
ユーザデバイス側制御部
(上位Software)
③利用命令(AC)
①利用要求
⑤相互認証
280
デコーダ(Decoder)
⑦Content Key復号
⑩Content復号
⑨Content復号命令
222
②AC検索
⑧Content検索
AC
Content

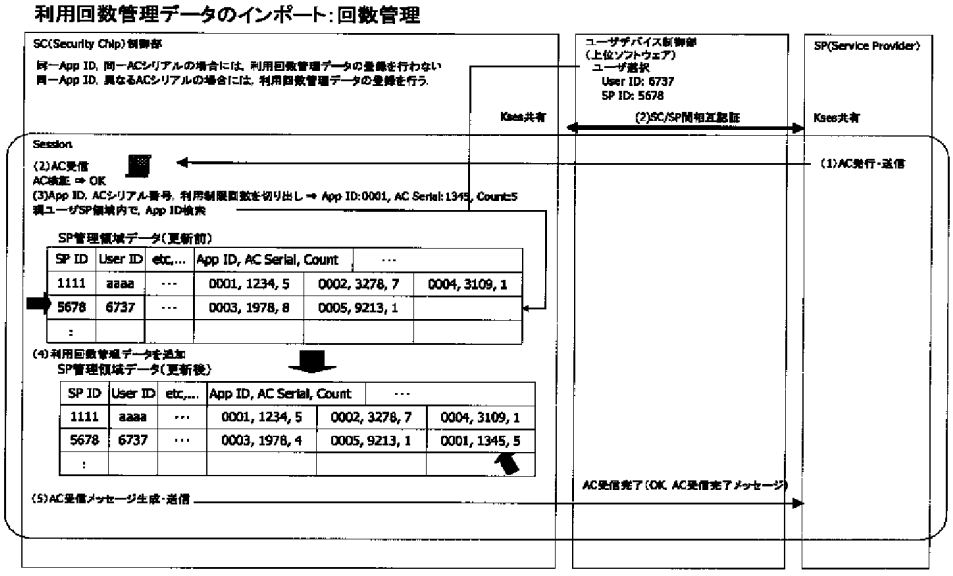
【図３１】


セキュリティチップ
ユーザデバイス側制御部
(上位Software)
デコーダ
利用者による
コンテンツ選択
上位Software
によるAppIDの取得
上位Software
によるAC検索
HSDによるAC検証
Content Keyの復号
上位Softwareから
HSDに対しAC検証
命令を発行
上位Softwareは、
HSDからの応答を
受信
上位Software仲介
による相互認証
Content Keyの
セッション鍵による
再暗号化
Content Keyの送信
Content Keyの
セッション鍵による
復号化
上位Software
によるContent検索
上位Software
からContent送信
Content Keyによる
Contentの復号化

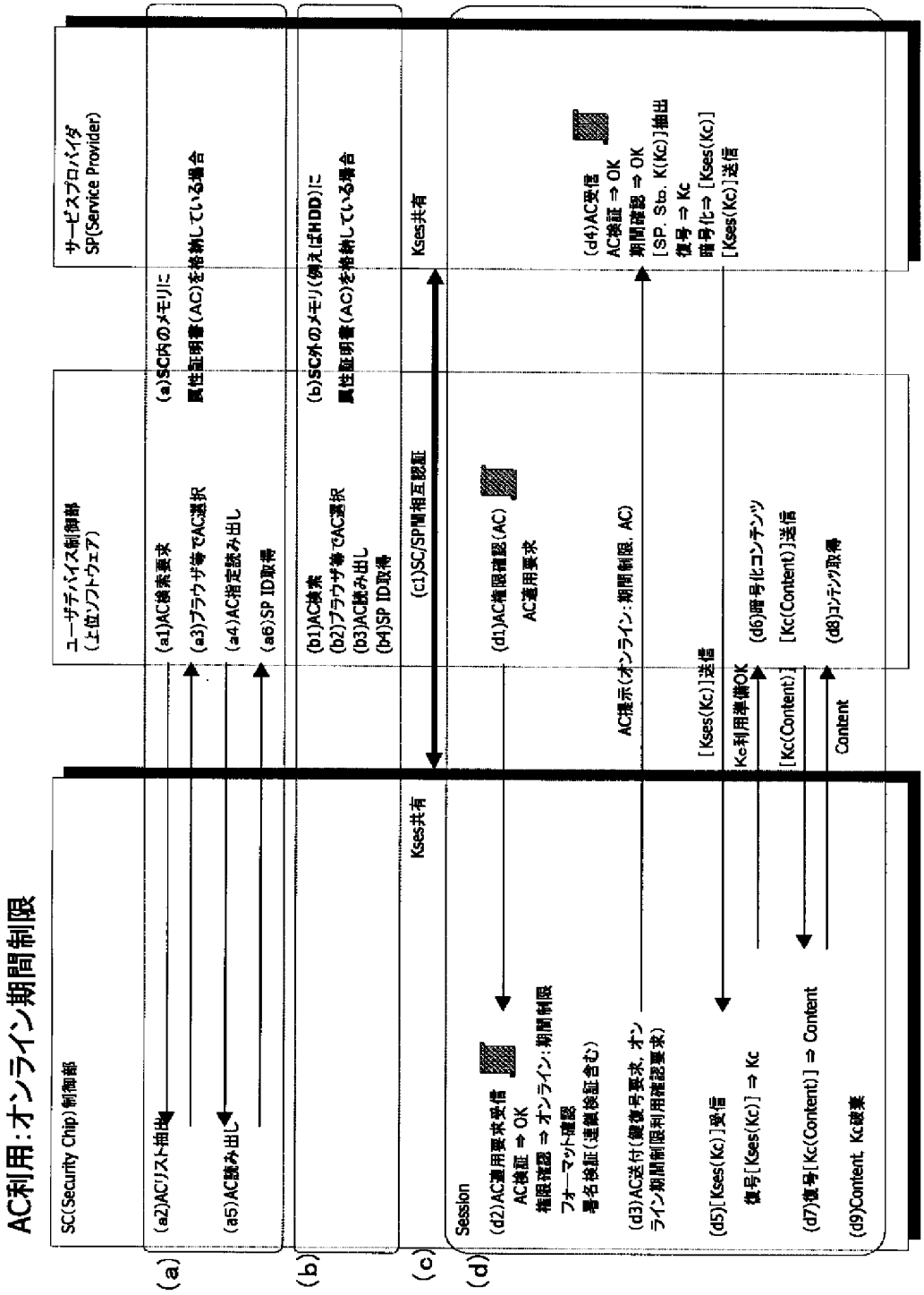
【図３２】


スタート
S101
利用者による
コンテンツ選択
S102
上位Software
によるAppIDの取得
S103
上位Software
によるAC検索
S104
上位SoftwareからHSDに対しAC検証命令を発行
S106
HSDによるAC検証
Content Keyの復号
S106
上位Softwareは、
HSDからの応答を受信
S107
検証成功か？
NG
OK
エラー
S108
上位SoftwareからHSDに対し第1認証コマンドを発行
S109
上位Softwareは、HSDからの応答を受信
S110
上位Softwareは、Decoderに第2認証コマンドを発行
S111
上位Softwareは、Decoderからの応答を受信
S112
上位SoftwareからHSDに対し第3認証コマンドを発行
S113
上位Softwareは、HSDからの応答を受信
S114
認証成功か？
NG
OK
エラー
S115
上位Softwareは、Decoderに第4認証コマンドを発行
S116
上位Softwareは、Decoderからの応答を受信
S117
認証成功か？
NG
OK
S118
HSDは、セッション鍵でContent Keyを再暗号化
S119
上位Softwareは、HSDからContent Keyを受信
S120
上位Softwareは、DecoderにContent Keyを送信
S121
Decoderは、セッション鍵でContent Keyを復号化
S122
上位SoftwareによるContent検索
S123
上位SoftwareからDecoderにContentを送信
S124
Decoderは Content KeyでContentを復号化
終了

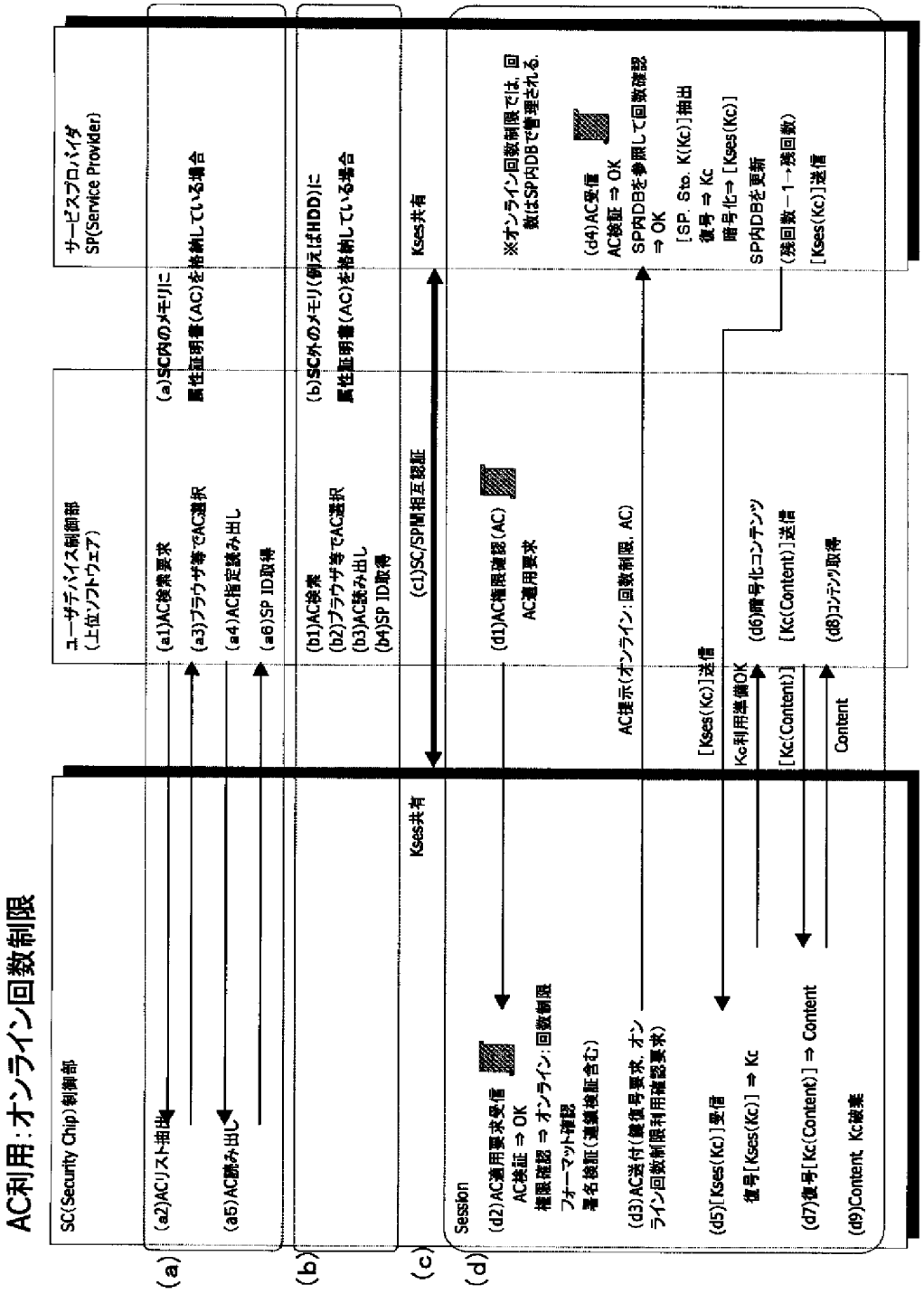
【図３７】


利用回数管理データのインポート：回数管理
SC(Security Chip)制御部
同一App ID, 同一ACシリアルの場合には、利用回数管理データの登録を行わない
同一App ID, 異なるACシリアルの場合には、利用回数管理データの登録を行う.
ユーザデバイス制御部
(上位ソフトウェア)
ユーザ選択
User ID: 6737
SP ID: 5678
SP(Service Provider)
Kaes共有
(2)SC/SP間相互認証
Kaes共有
Session
(2)AC受信
AC検証 ⇒ OK
(1)AC発行・送信
(3)App ID, ACシリアル番号, 利用制限回数を切り出し ⇒ App ID:0001, AC Serial:1345, Count:5
該ユーザSP領域内で, App ID検索
SP管理領域データ(更新前)
SP ID | User ID | etc,... | App ID, AC Serial, Count | ...
1111 | aaaa | ... | 0001, 1234, 5 | 0002, 3278, 7 | 0004, 3109, 1
5678 | 6737 | ... | 0003, 1978, 8 | 0005, 9213, 1
:
(4)利用回数管理データを追加
SP管理領域データ(更新後)
SP ID | User ID | etc,... | App ID, AC Serial, Count | ...
1111 | aaaa | ... | 0001, 1234, 5 | 0002, 3278, 7 | 0004, 3109, 1
5678 | 6737 | ... | 0003, 1978, 4 | 0005, 9213, 1 | 0001, 1345, 5
:
AC受信完了(OK, AC受信完了メッセージ)
(5)AC受信メッセージ生成・送信

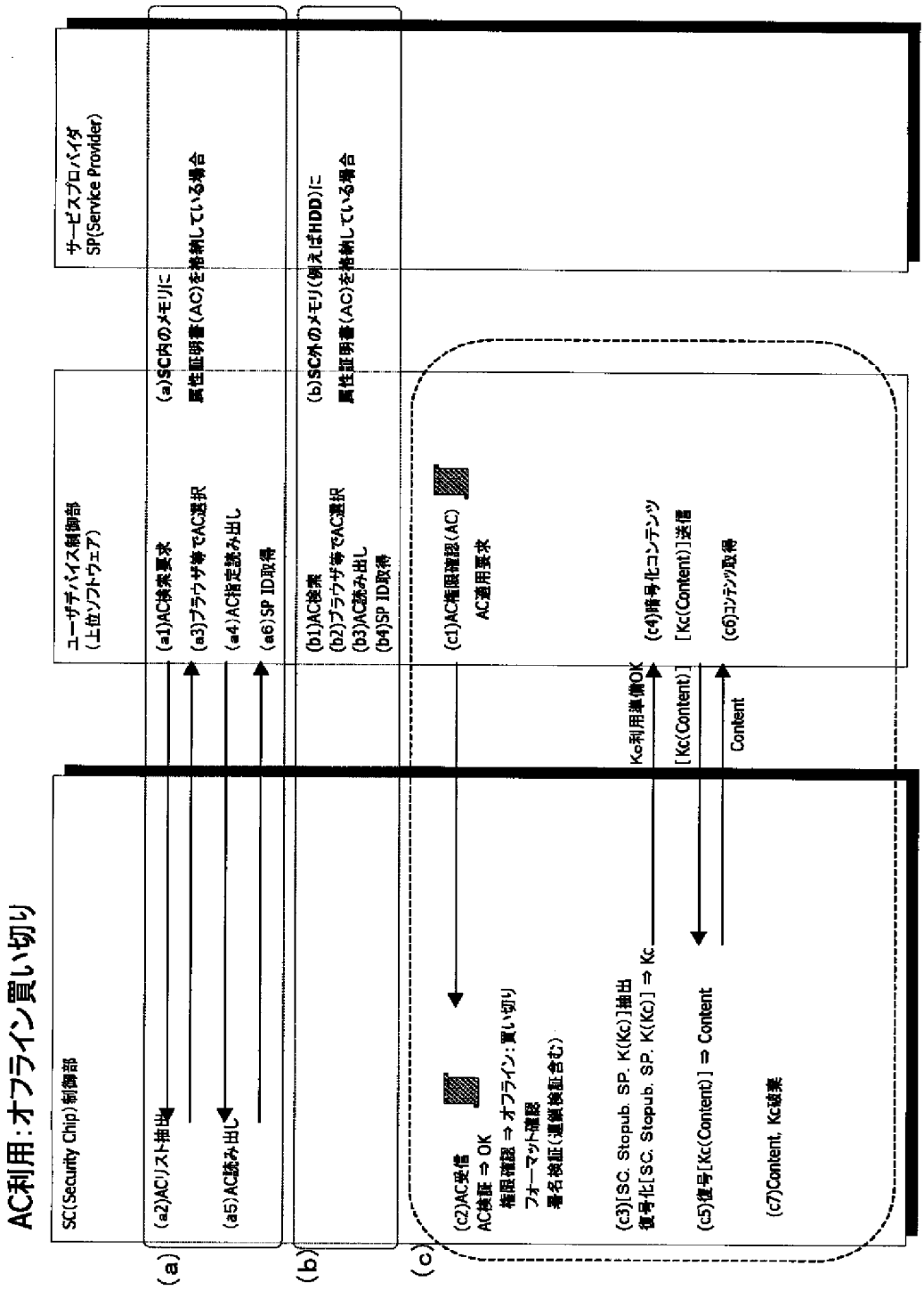
【図３４】


AC利用:オンライン期間制限
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内のメモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)SC/SP間相互認証
Kses共有
Kses共有
(d1)AC権限確認(AC)
AC運用要求
(d2)AC運用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン:期間制限
フォーマット確認
署名検証(連鎖検証含む)
(d3)AC送付(鍵復号要求, オンライン期間制限利用確認要求)
AC提示(オンライン:期間制限, AC)
(d4)AC受信
AC検証 ⇒ OK
期間確認 ⇒ OK
[SP, Sto, K(Kc)]抽出
復号 ⇒ Kc
暗号化⇒ [Kses(Kc)]
[Kses(Kc)]送信
[Kses(Kc)]送信
(d5)[Kses(Kc)]受信
復号[Kses(Kc)] ⇒ Kc
Kc利用準備OK
(d6)暗号化コンテンツ
[Kc(Content)]送信
[Kc(Content)]
(d7)復号[Kc(Content)] ⇒ Content
Content
(d8)コンテンツ取得
(d9)Content, Kc破棄
Session

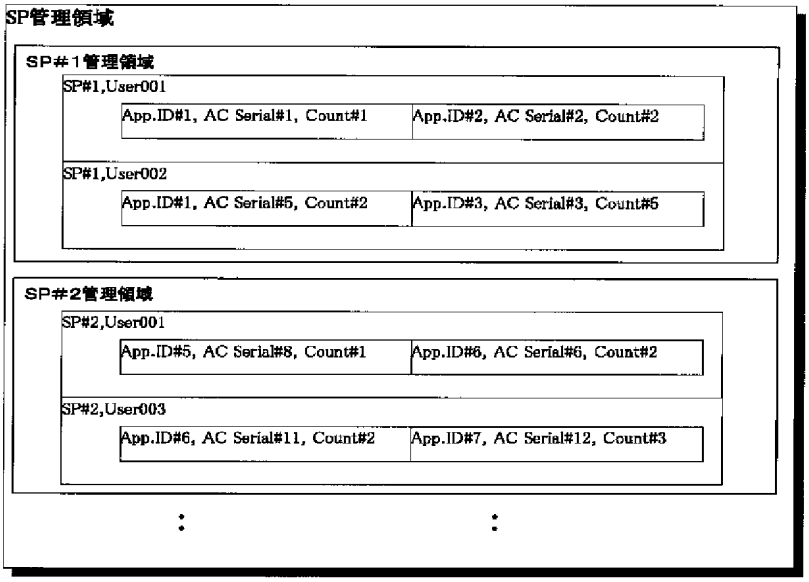
【図３５】


AC利用：オンライン回数制限
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a2)ACリスト抽出
(a1)AC検索要求
(a)SC内のメモリに
(a3)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(a5)AC読み出し
(a4)AC指定読み出し
(a6)SP ID取得
(b1)AC検索
(b)SC外のメモリ(例えばHDD)に
(b2)ブラウザ等でAC選択
(b3)AC読み出し
属性証明書(AC)を格納している場合
(b4)SP ID取得
(c1)SC/SP間相互認証
Kses共有
Kses共有
※オンライン回数制限では，回数はSP内DBで管理される．
(d4)AC受信
AC検証 ⇒ OK
SP内DBを参照して回数確認
⇒ OK
[SP. Sto. K(Kc)]抽出
復号 ⇒ Kc
暗号化⇒ [Kses(Kc)]
SP内DBを更新
(残回数－1→残回数)
[Kses(Kc)]送信
Session
(d2)AC適用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン：回数制限
フォーマット確認
署名検証(連鎖検証含む)
(d1)AC権限確認(AC)
AC適用要求
(d3)AC送付(復号号要求，オンライン回数制限利用確認要求)
AC提示(オンライン：回数制限，AC)
(d5)[Kses(Kc)]受信
復号[Kses(Kc)] ⇒ Kc
[Kses(Kc)]送信
Kc利用準備OK
(d6)暗号化コンテンツ
[Kc(Content)]送信
(d7)復号[Kc(Content)] ⇒ Content
[Kc(Content)]
(d8)コンテンツ取得
Content
(d9)Content, Kc破棄

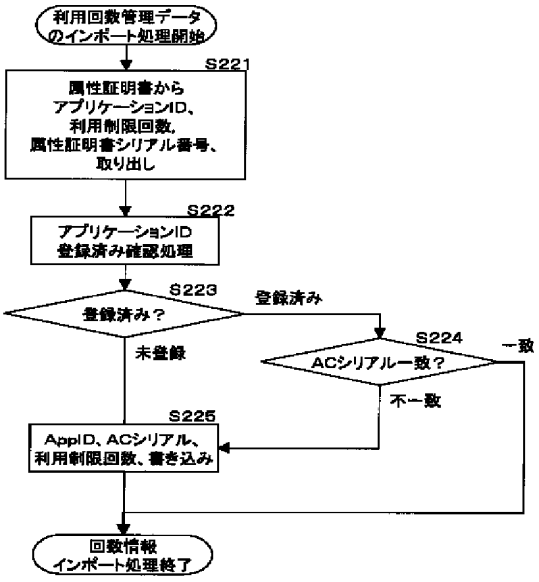
【図３６】


AC利用:オフライン買い切り
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内のメモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)AC権限確認(AC)
AC適用要求
(c2)AC受信
AC検証 ⇒ OK
権限確認 ⇒ オフライン:買い切り
フォーマット確認
署名検証(連鎖検証含む)
(c3)[SC. Stapub. SP. K(Kc)]抽出
復号化[SC. Stapub. SP. K(Kc)] ⇒ Kc
(c4)暗号化コンテンツ
[Kc(Content)]送信
(c5)復号[Kc(Content)] ⇒ Content
(c6)コンテンツ取得
(c7)Content, Kc破棄
Kc利用準備OK
[Kc(Content)]
Content

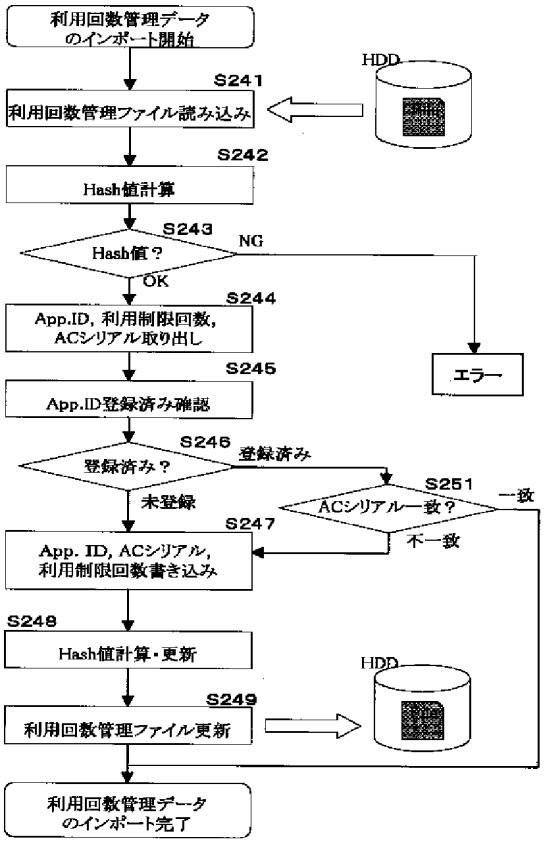
【図３８】


SP管理領域
SP#1管理領域
SP#1,User001
App.ID#1, AC Serial#1, Count#1
App.ID#2, AC Serial#2, Count#2
SP#1,User002
App.ID#1, AC Serial#5, Count#2
App.ID#3, AC Serial#3, Count#5
SP#2管理領域
SP#2,User001
App.ID#5, AC Serial#8, Count#1
App.ID#6, AC Serial#6, Count#2
SP#2,User003
App.ID#6, AC Serial#11, Count#2
App.ID#7, AC Serial#12, Count#3

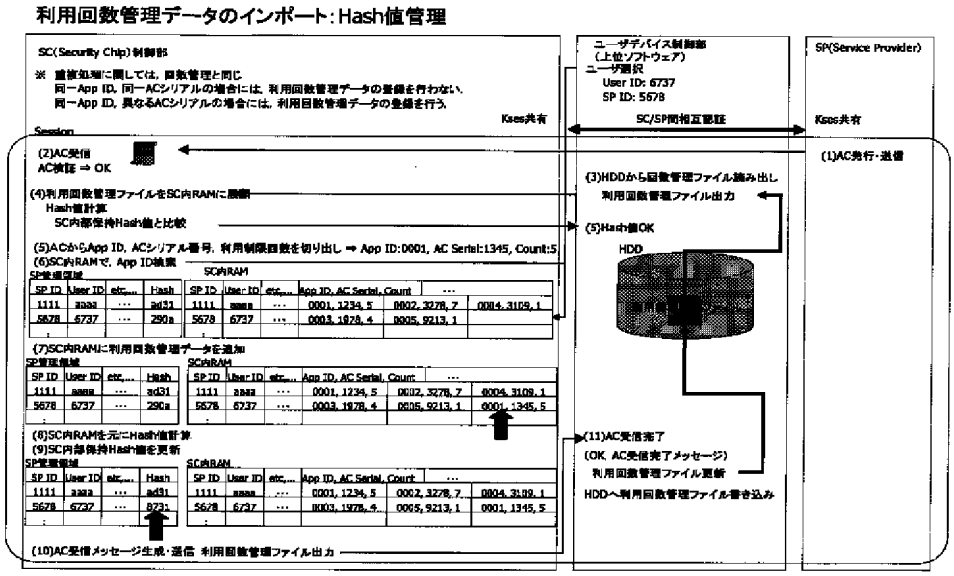
【図３９】


利用回数管理データのインポート処理開始
S221
属性証明書からアプリケーションID、利用制限回数、属性証明書シリアル番号、取り出し
S222
アプリケーションID登録済み確認処理
S223
登録済み？
登録済み
未登録
S224
ACシリアル一致？
一致
不一致
S225
AppID、ACシリアル、利用制限回数、書き込み
回数情報インポート処理終了

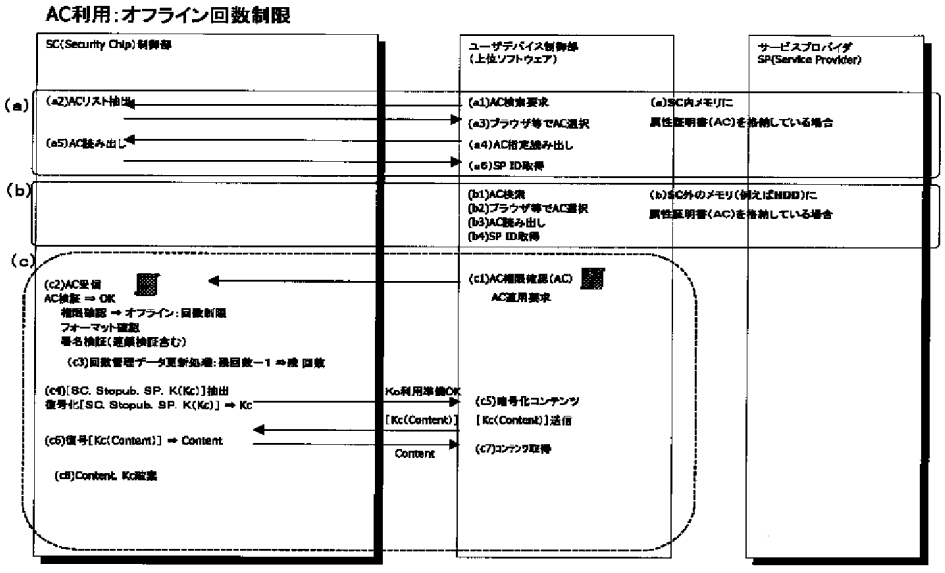
【図４１】


利用回数管理データのインポート開始
HDD
S241
利用回数管理ファイル読み込み
S242
Hash値計算
S243
Hash値？
NG
OK
エラー
S244
App.ID, 利用制限回数, ACシリアル取り出し
S245
App.ID登録済み確認
S246
登録済み？
登録済み
未登録
S251
ACシリアル一致？
一致
不一致
S247
App. ID, ACシリアル, 利用制限回数書き込み
S248
Hash値計算・更新
HDD
S249
利用回数管理ファイル更新
利用回数管理データのインポート完了

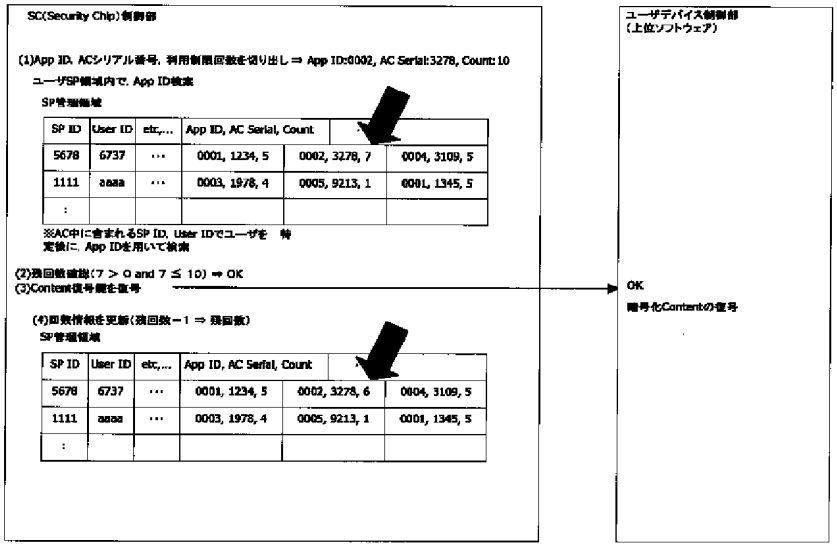
【図４０】


利用回数管理データのインポート：Hash値管理
SC(Security Chip)制御部
※ 重複処理に関しては，回数管理と同じ
同一App ID，同一ACシリアルの場合には，利用回数管理データの登録を行わない．
同一App ID，異なるACシリアルの場合には，利用回数管理データの登録を行う．
Kses共有
Session
(2)AC受信
AC検証 ⇒ OK
(4)利用回数管理ファイルをSC内RAMに展開
Hash値計算
SC内部保持Hash値と比較
(5)ACからApp ID，ACシリアル番号，利用制限回数を切り出し ⇒ App ID:0001, AC Serial:1345, Count:5
(6)SC内RAMで，App ID検索
SC内RAM
(7)SC内RAMに利用回数管理データを追加
SC内RAM
(8)SC内RAMを元にHash値計算
(9)SC内部保持Hash値を更新
SC内RAM
(10)AC受信メッセージ生成・送信 利用回数管理ファイル出力
ユーザデバイス制御部
（上位ソフトウェア）
ユーザ選択
User ID: 6737
SP ID: 5678
SC/SP間相互認証
(3)HDDから回数管理ファイル読み出し
利用回数管理ファイル出力
(5)Hash値OK
HDD
(11)AC受信完了
(OK, AC受信完了メッセージ)
利用回数管理ファイル更新
HDDへ利用回数管理ファイル書き込み
SP(Service Provider)
Kses共有
(1)AC発行・送信

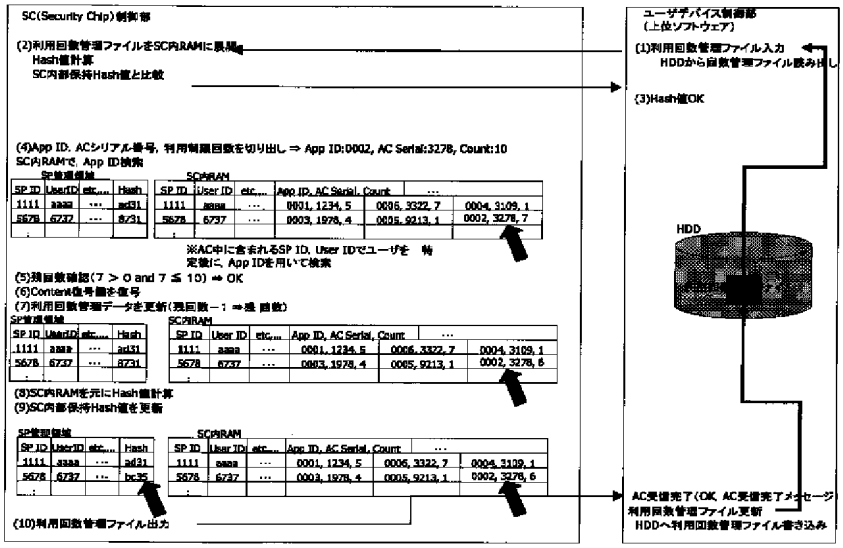
【図４２】


AC利用：オフライン回数制限
SC(Security Chip)制御部
ユーザデバイス制御部
（上位ソフトウェア）
サービスプロバイダ
SP(Service Provider)
(a)
(a2)ACリスト抽出
(a5)AC読み出し
(a1)AC検索要求
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a6)SP ID取得
(a)SC内メモリに
属性証明書(AC)を格納している場合
(b)
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c)
(c2)AC受信
AC検証 ⇒ OK
権限確認 ⇒ オフライン：回数制限
フォーマット確認
署名検証(証明検証含む)
(c3)回数管理データ更新処理：残回数－1 ⇒新 回数
(c4)[SC. Stopub. SP. K(Kc)]抽出
復号化[SC. Stopub. SP. K(Kc)] ⇒ Kc
(c6)復号[Kc(Content)] ⇒ Content
(c8)Content, Kc格納
(c1)AC権限確認(AC)
AC運用要求
Kc利用準備OK
(c5)暗号化コンテンツ
[Kc(Content)]
[Kc(Content)]送信
Content
(c7)コンテンツ取得

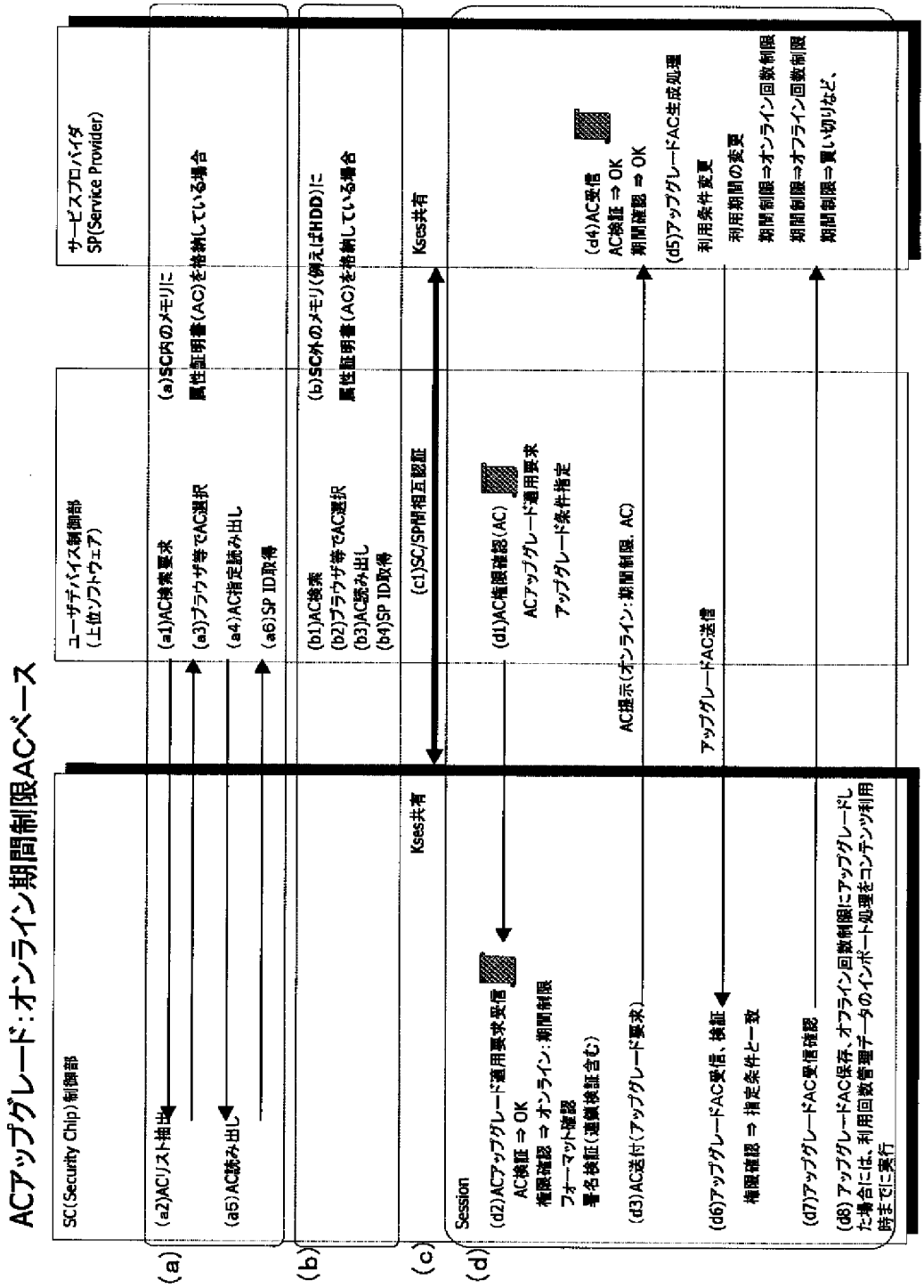
【図４３】


利用回数管理データの更新：回数管理
SC(Security Chip)制御部
(1)App ID, ACシリアル番号, 利用制限回数を切り出し ⇒ App ID:0002, AC Serial:3278, Count:10
ユーザSP領域内で, App IDを検索
SP管理領域
SP ID
User ID
etc,...
App ID, AC Serial, Count
5678
6737
0001, 1234, 5
0002, 3278, 7
0004, 3109, 5
1111
aaaa
0003, 1978, 4
0005, 9213, 1
0001, 1345, 5
※AC中に含まれるSP ID, User IDでユーザを　特
定後に, App IDを用いて検索
(2)残回数確認(7 > 0 and 7 ≦ 10) ⇒ OK
(3)Content復号鍵を復号
(4)回数情報を更新(残回数－1 ⇒ 残回数)
SP管理領域
0002, 3278, 6
0003, 1978, 4
0005, 9213, 1
0001, 1345, 5
ユーザデバイス制御部
(上位ソフトウェア)
OK
暗号化Contentの復号

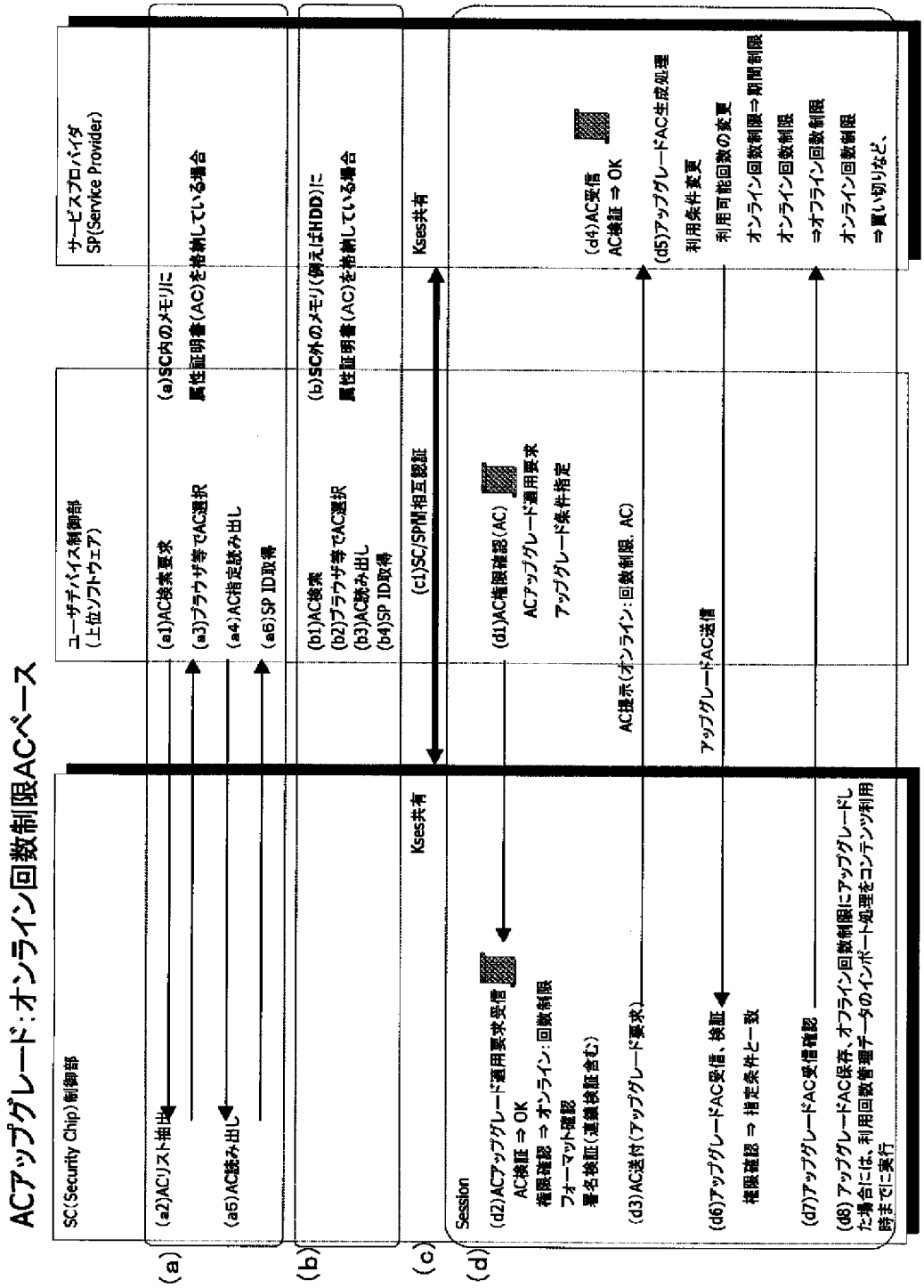
【図４４】


利用回数管理データの更新：Hash値管理
SC(Security Chip)制御部
(2)利用回数管理ファイルをSC内RAMに展開
Hash値計算
SC内部保持Hash値と比較
(4)App ID, ACシリアル番号, 利用制限回数を切り出し ⇒ App ID:0002, AC Serial:3278, Count:10
SC内RAMで, App ID検索
SP管理領域
SC内RAM
SP ID
UserID
etc,...
Hash
App ID, AC Serial, Count
1111
aaaa
ad31
5678
6737
8731
0001, 1234, 5
0006, 3322, 7
0004, 3109, 1
0003, 1978, 4
0005, 9213, 1
0002, 3278, 7
※AC中に含まれるSP ID, User IDでユーザを　特
定後に, App IDを用いて検索
(5)残回数確認(7 > 0 and 7 ≦ 10) ⇒ OK
(6)Content復号鍵を復号
(7)利用回数管理データを更新(残回数－1 ⇒残 回数)
(8)SC内RAMを元にHash値計算
(9)SC内部保持Hash値を更新
bc35
(10)利用回数管理ファイル出力
ユーザデバイス制御部
(上位ソフトウェア)
(1)利用回数管理ファイル入力
HDDから回数管理ファイル読み出し
(3)Hash値OK
HDD
AC受信完了(OK, AC受信完了メッセージ
利用回数管理ファイル更新
HDDへ利用回数管理ファイル書き込み

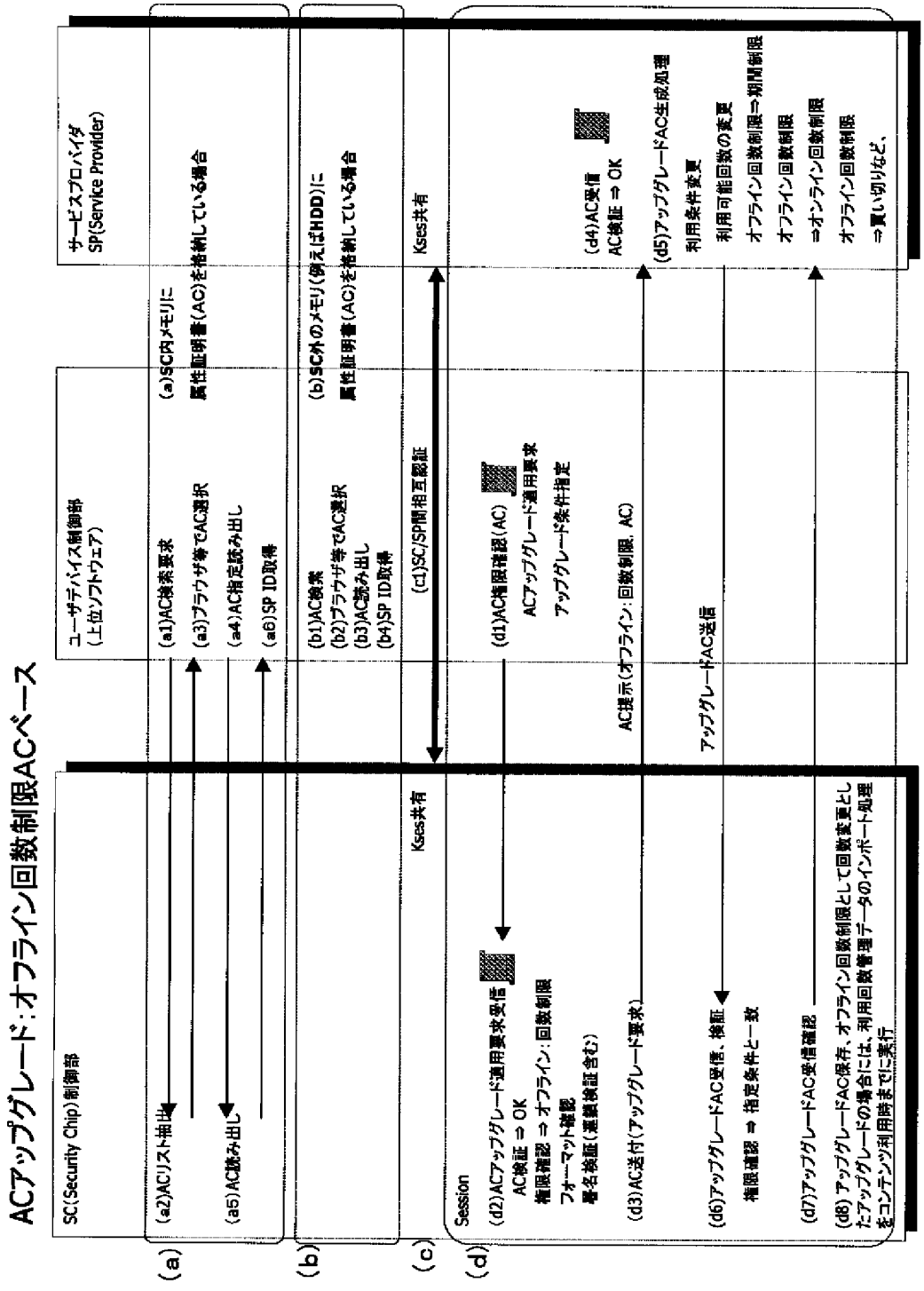
【図４５】


ACアップグレード:オンライン期間制限ACベース
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a)SC内のメモリに
(a2)AC(リスト)抽出
(a3)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(b1)AC検索
(b)SC外のメモリ(例えばHDD)に
(b2)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(b3)AC読み出し
(b4)SP ID取得
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
ACアップグレード適用要求
アップグレード条件指定
(d2)ACアップグレード適用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン:期間制限
フォーマット確認
署名検証(連鎖検証含む)
(d3)AC送付(アップグレード要求)
AC提示(オンライン:期間制限, AC)
(d4)AC受信
AC検証 ⇒ OK
期間確認 ⇒ OK
(d5)アップグレードAC生成処理
利用条件変更
利用期間の変更
期間制限⇒オンライン回数制限
期間制限⇒オフライン回数制限
期間制限⇒買い切りなど、
アップグレードAC送信
(d6)アップグレードAC受信、検証
権限確認 ⇒ 指定条件と一致
(d7)アップグレードAC受信確認
(d8) アップグレードAC保存. オフライン回数制限にアップグレードした場合には、利用回数管理データのインポート処理をコンテンツ利用時までに実行

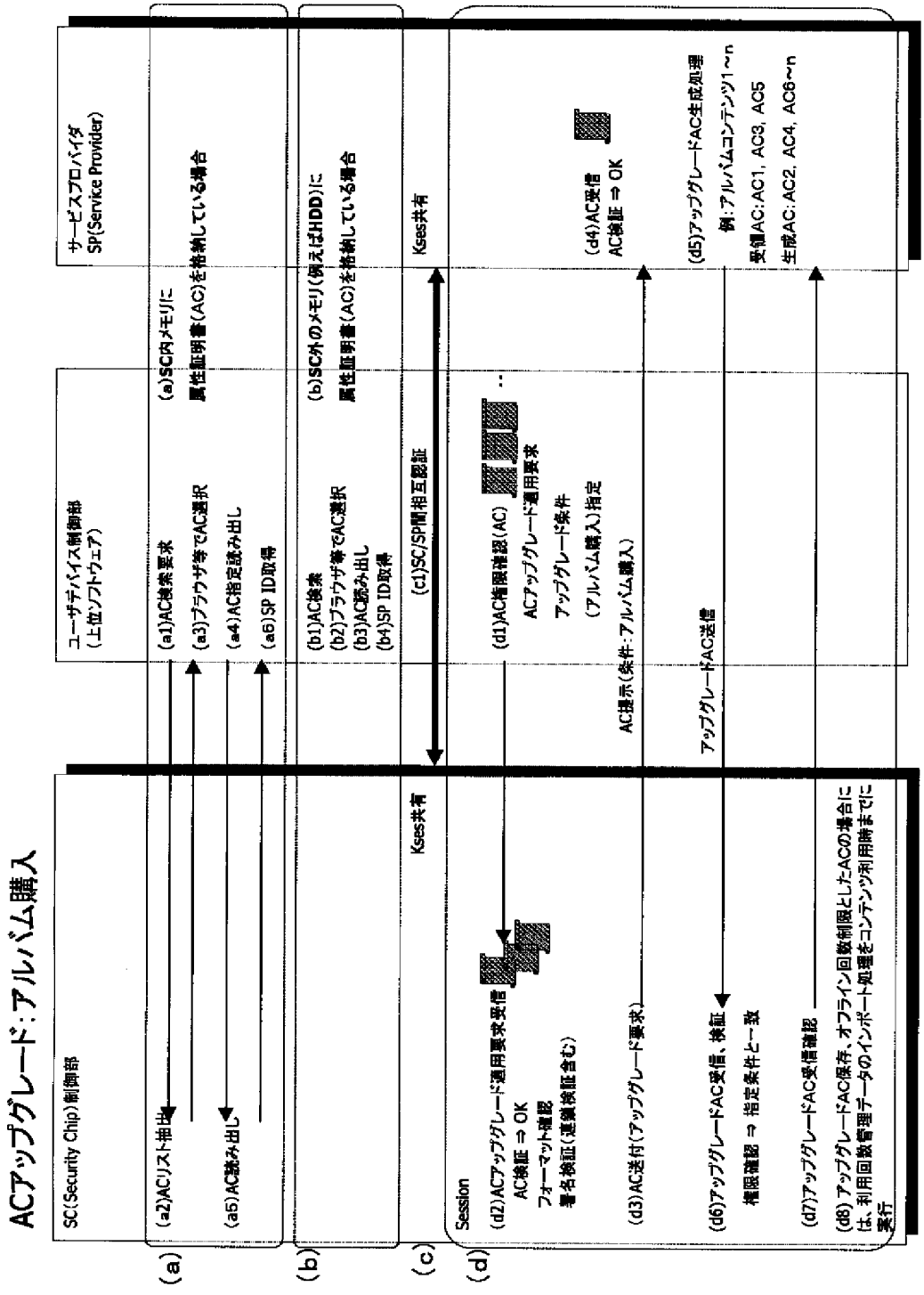
【図４６】


ACアップグレード:オンライン回数制限ACベース
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内のメモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
ACアップグレード適用要求
アップグレード条件指定
(d2)ACアップグレード適用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン:回数制限
フォーマット確認
署名検証(連鎖検証含む)
(d3)AC送付(アップグレード要求)
AC提示(オンライン:回数制限, AC)
(d4)AC受信
AC検証 ⇒ OK
(d5)アップグレードAC生成処理
利用条件変更
アップグレードAC送信
(d6)アップグレードAC受信、検証
権限確認 ⇒ 指定条件と一致
利用可能回数の変更
オンライン回数制限⇒期間制限
オンライン回数制限
⇒オフライン回数制限
(d7)アップグレードAC受信確認
(d8) アップグレードAC保存. オフライン回数制限にアップグレードした場合には、利用回数管理データのインポート処理をコンテンツ利用時までに実行
オンライン回数制限
⇒買い切りなど、

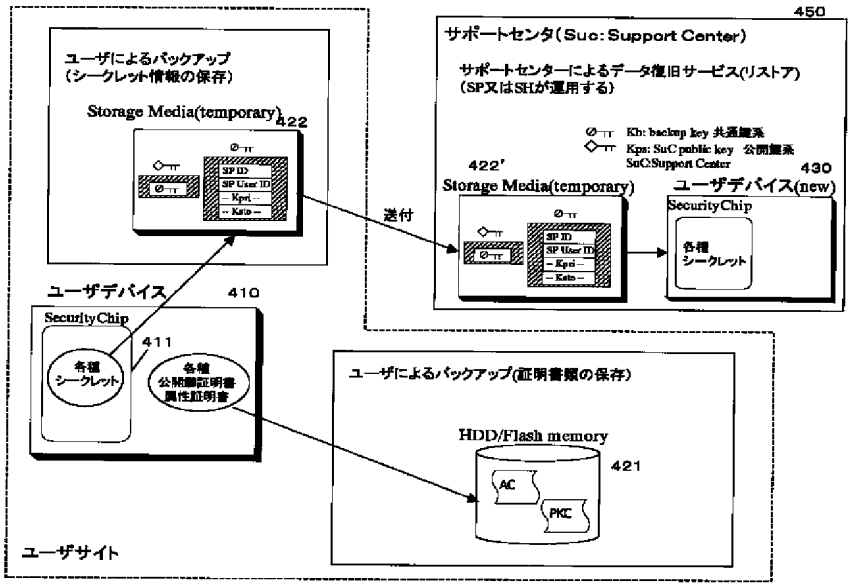
【図４７】


ACアップグレード:オフライン回数制限ACベース
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a)SC内メモリに
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(b1)AC検索
(b)SC外のメモリ(例えばHDD)に
(b2)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(b3)AC読み出し
(b4)SP ID取得
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
ACアップグレード適用要求
アップグレード条件指定
(d2)ACアップグレード適用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オフライン:回数制限
フォーマット確認
署名検証(連鎖検証含む)
(d3)AC送付(アップグレード要求)
AC提示(オフライン:回数制限, AC)
(d4)AC受信
AC検証 ⇒ OK
(d5)アップグレードAC生成処理
利用条件変更
利用可能回数の変更
アップグレードAC送信
(d6)アップグレードAC受信、検証
権限確認 ⇒ 指定条件と一致
オフライン回数制限⇒期間制限
オフライン回数制限
⇒オンライン回数制限
(d7)アップグレードAC受信確認
オフライン回数制限
⇒買い切りなど、
(d8) アップグレードAC保存. オフライン回数制限として回数変更とした
アップグレードの場合には、利用回数管理データのインポート処理
をコンテンツ利用時までに実行

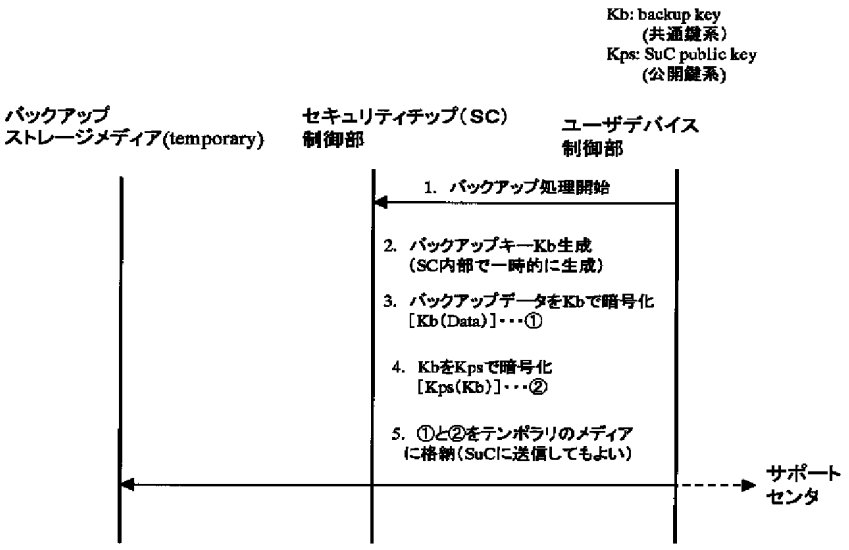
【図４８】


ACアップグレード：アルバム購入
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内メモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
ACアップグレード運用要求
アップグレード条件
(アルバム購入)指定
(d2)ACアップグレード運用要求受信
AC検証 ⇒ OK
フォーマット確認
署名検証(連鎖検証含む)
AC提示(条件:アルバム購入)
(d3)AC送付(アップグレード要求)
(d4)AC受信
AC検証 ⇒ OK
アップグレードAC送信
(d5)アップグレードAC生成処理
例:アルバムコンテンツ1～n
受領AC:AC1, AC3, AC5
生成AC:AC2, AC4, AC6～n
(d6)アップグレードAC受信、検証
権限確認 ⇒ 指定条件と一致
(d7)アップグレードAC受信確認
(d8)アップグレードAC保存、オフライン回数制限としたACの場合には、利用回数管理データのインポート処理をコンテンツ利用開始までに実行

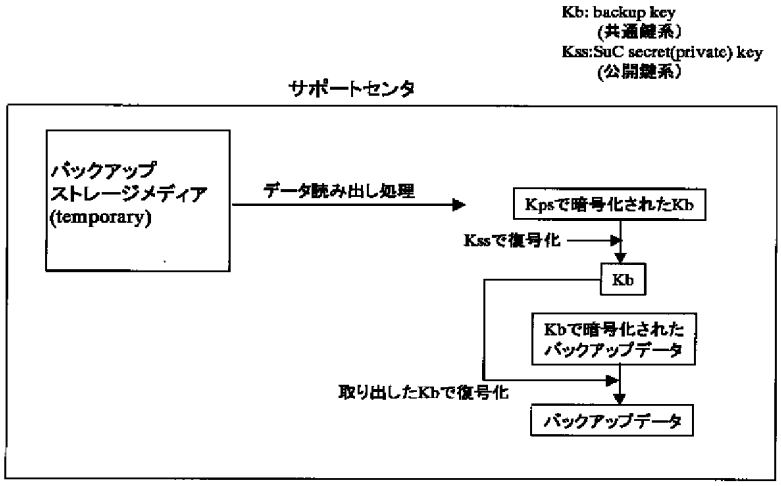
【図４９】


450
サポートセンタ(Suc: Support Center)
サポートセンターによるデータ復旧サービス(リストア)
(SP又はSHが運用する)
Kb: backup key 共通鍵系
Kps: SuC public key 公開鍵系
SuC:Support Center
430
422'
Storage Media(temporary)
ユーザデバイス(new)
SecurityChip
各種
シークレット
送付
ユーザによるバックアップ
(シークレット情報の保存)
Storage Media(temporary)
422
SP ID
SP User ID
Kpri
Kstb
ユーザデバイス
410
SecurityChip
411
各種
シークレット
各種
公開鍵証明書
属性証明書
ユーザによるバックアップ(証明書類の保存)
HDD/Flash memory
421
AC
PKC
ユーザサイト

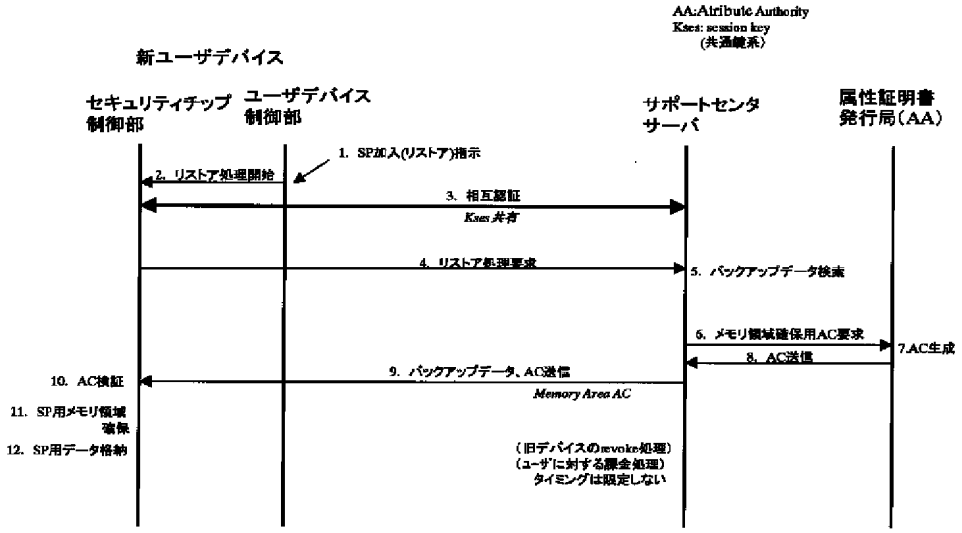
【図５１】


Kb: backup key
(共通鍵系)
Kps: SuC public key
(公開鍵系)
バックアップ
ストレージメディア(temporary)
セキュリティチップ(SC)
制御部
ユーザデバイス
制御部
1. バックアップ処理開始
2. バックアップキーKb生成
(SC内部で一時的に生成)
3. バックアップデータをKbで暗号化
[Kb(Data)]・・・①
4. KbをKpsで暗号化
[Kps(Kb)]・・・②
5. ①と②をテンポラリのメディア
に格納(SuCに送信してもよい)
サポート
センタ

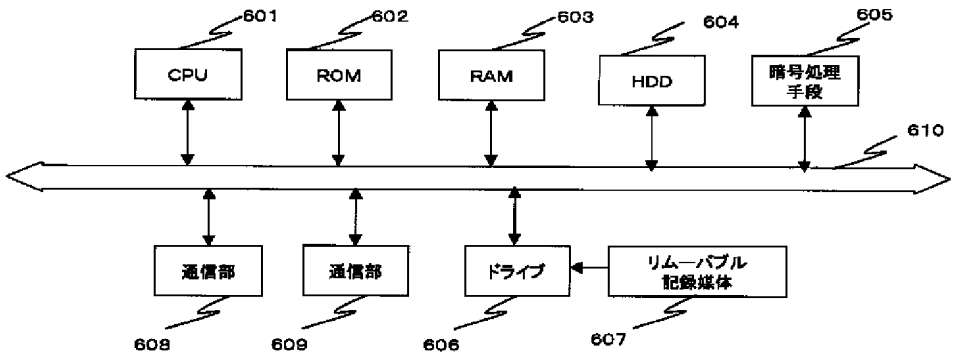
【図５２】


Kb: backup key
(共通鍵系)
Kss:SuC secret(private) key
(公開鍵系)
サポートセンタ
バックアップ
ストレージメディア
(temporary)
データ読み出し処理
Kpsで暗号化されたKb
Kssで復号化
Kb
Kbで暗号化された
バックアップデータ
取り出したKbで復号化
バックアップデータ

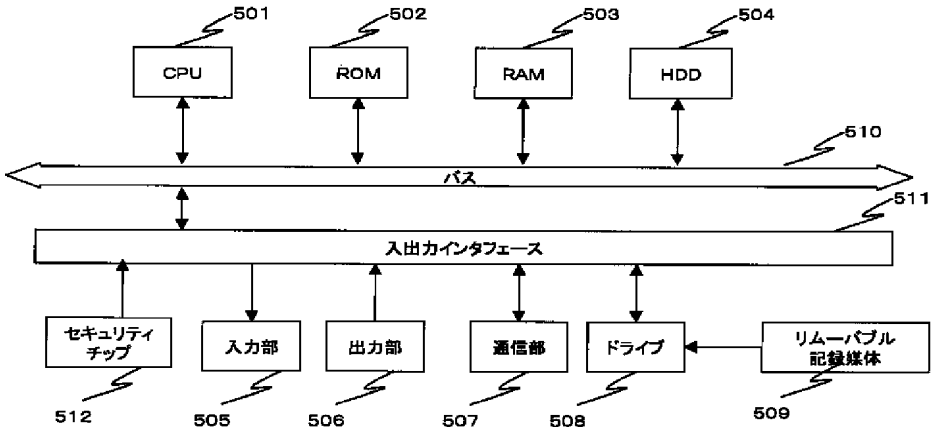
【図５３】


AA:Attribute Authority
Kses: session key
(共通鍵系)
新ユーザデバイス
セキュリティチップ
制御部
ユーザデバイス
制御部
サポートセンタ
サーバ
属性証明書
発行局(AA)
1. SP加入(リストア)指示
2. リストア処理開始
3. 相互認証
Kses 共有
4. リストア処理要求
5. バックアップデータ検索
6. メモリ領域確保用AC要求
7.AC生成
8. AC送信
9. バックアップデータ、AC送信
Memory Area AC
10. AC検証
11. SP用メモリ領域
確保
12. SP用データ格納
(旧デバイスのrevoke処理)
(ユーザに対する課金処理)
タイミングは限定しない

【図５５】


601
602
603
604
605
CPU
ROM
RAM
HDD
暗号処理
手段
610
通信部
通信部
ドライブ
リムーバブル
記録媒体
608
609
606
607

【図５４】



フロントページの続き

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ (参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６０１Ｅ
			６７５Ｂ

(72)発明者　阿部　博
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　岡　誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA03 BA07 CA16
5B018 GA04 HA05 KA22 MA12 NA06
5B082 DE02
5J104 AA07 AA16 EA05 EA06 EA19
KA02 NA02 NA05 NA12 NA35
NA36 NA37 NA42 PA07